

# TERENA Technical Report

## Middleware Activity Report



### Authentication, Authorisation and Roaming

Licia Florio  
September 2005

# TERENA Middleware Activity Report

The aim of this report is to provide an overview of the TERENA activities in the middleware arena. Middleware activities are carried out by two task forces that operated under the auspices of the TERENA Technical Programme.

The Task Force EMC2 (European Middleware Coordination and Collaboration) is a middleware forum for Europe and beyond.

The task force TF-Mobility focuses especially on authentication to wireless LANs, complementing the work of TF-EMC2.

This report focuses on the results achieved by these two task-forces, covering a period of one year (September 2004 – September 2005).

## **For Further information please contact:**

TERENA Secretariat  
Singel 468 D  
1017 AW Amsterdam  
The Netherlands

Tel: +31 20 530 4488  
Fax: +31 20 530 4499  
E-mail: [secretariat@terena.nl](mailto:secretariat@terena.nl)  
www: <http://www.terena.nl>

© TERENA 2005 All rights reserved

Parts of this report may be freely copied, unaltered, provided that the original source is acknowledged and the copyright preserved.

Production: TERENA Secretariat

# TERENA Middleware Activity Report

## TF-EMC2: history, status and future

(Task Force European Middleware Coordination and Collaboration)

<http://www.terena.nl/tech/task-forces/tf-emc2/>

### Introduction

The TERENA Task Force EMC2 is the follow up of a previous task force called TF-AACE, terminated in 2004 and focused on Authentication and Authorisation (AA) issues.

TF-AACE gathered a lot of interest among the NRENs in Europe and the Internet2 community. One of the recommendations of TF-AACE was to set-up a new task force with a broader focus than just authentication and authorisation.

This reflected the fact that the initial idea of building a common AA system developed into the concept of keeping the various AA systems already in use in different NRENs and enabling them to inter-operate amongst each other. The need of interoperability has led to development of different pieces of software known as middleware, where of course authentication and authorisation play an important role.

### TF-EMC2 aims and relation with GEANT2-JRA5

TF-EMC2, whose mandate started in September 2004, spans over a wider area than just authentication and authorisation, covering what is identified as middleware and also aims to provide feedback to ongoing initiatives started under TF-AACE.

When the charter of the task force was under preparation it was agreed to keep the list of working items open, selecting some items of immediate interest in the NRENs community, but leaving the possibility to add new items whenever required.

The task force is chaired by Diego Lopez from RedIRIS and includes the participation of most of the NRENs in Europe, Internet2 and other organisation operating in high energy physics.

TF-EMC2 liaises closely with the GN2 Joint Research Activity 5 “Roaming and Authorisation” (JRA5), which started its work building on the former TF-AACE and TF-Mobility<sup>1</sup> results in order to define, prototype and build a roaming infrastructure first and then an authentication and authorisation infrastructure (AAI) for European academic and research institutions.

TF-EMC2 and JRA5 operates as two different groups, with some people active in both.

---

<sup>1</sup> For more details see TF-Mobility section of this report.

# TERENA Middleware Activity Report

TF-EMC2 provides a dissemination and discussion forum about the progresses of the JRA5 group (which is a closed group) as well as a technical support for possible emerging technologies related to the middleware area. However TF-EMC2 has a broader scope than JRA5, taking also into account the international context which goes beyond Europe.

The following five working items have been identified in the charter of TF-EMC2:

1. Authentication and Authorisation Requester-Responder
2. TACAR
3. Campus Middleware Issues
4. Directory - schema
5. Other TF-EMC2 related activities

## **1. Authentication and Authorisation Requester-Responder**

<http://www.terena.nl/tech/task-forces/tf-emc2/aarr.html>

AA-RR (Authentication and Authorization Requester-Responder) is a tool, developed by RedIRIS. It is conceived to help in the validation of the interoperability of a certain AA components with other(s).

Whenever a new component is developed and has to be integrated in a given infrastructure, or two different infrastructures have somehow to be connected, there should be some assessment mechanisms in place to verify the compatibility of the new element into a system.

The main purpose of the AA-RR is the use of metadata describing the requirements of a certain infrastructure in order to validate (or make at least an assessment on) the interoperability of a certain component with other(s).

The first release of the AA-RR software was available during the last months of TF-AACE, but since then further development took place. The latest version of AA-RR, presented by Diego Lopez (RedIRIS) during the EMC2 meeting in June, supports different protocols, such as SAML and RADIUS as well as the SSO Spanish system PAPI. The AA-RR design offers an open framework for easily incorporating support for new protocols (such as A-Select and RADIUS).

# TERENA Middleware Activity Report

## 2. TACAR

(<http://www.tacar.org>)

The TERENA Academic Certification Authority Repository (TACAR) was established in 2003 to address the problem of the cross-domain use of the root CA certificates (trust anchors) of the various Certification Authorities (CAs) run by the NRENs.

The certificates collected by TACAR are those directly managed by NRENs or by institutions belonging either to a National Academic PKI in the TERENA member countries or to non-profit research projects.

TACAR provides an on-line trusted repository where an academic CA can register its trust anchor and the related CP/CPS. A policy document defines the procedure to register a root CA certificate.

Within TACAR trust is established by means of web of personal relationships among the participants in PKI-related initiatives co-ordinated by TERENA or in which TERENA participates.

The TACAR policy does not define procedures to analyse the policies of the different CAs and for this reason TACAR is not meant for final users. The idea the repository is based on is that the repository holds a centralised set of certificates and related policies so administrators in different locations know where to find a trust anchor, can evaluate the related policies and decide whether they want to trust a particular CA or not.

The process to include a root CA certificate into the repository is based on face-to-face meetings; however when the process has been started PGP keys can be used as a trusted way for electronic updates.

TERENA as the host organisation of the repository is responsible for undertaking the identification and authorisation procedure for an applying institution and for keeping the TACAR web site up-to-date.

The certificates are downloaded under https; since November 2004 the secure download makes use of a self-signed certificate, generated and maintained with the exclusive purpose of securing access to the repository.

The use of a self signed certificate is to warn the user to verify the finger print of the server certificate, as the certificate is not recognized by the browser (a pop-up window will appear at

# TERENA Middleware Activity Report

the moment of the user gets connected to the [www.tacar.org](http://www.tacar.org) web site). The finger print of this server self-signed certificate is:

**MD5** 10:AE:CE:44:A2:CC:15:C7:1D:71:61:6B:B5:70:AD:5C

**SHA1** F0:18:1C:A4:9C:7D:40:6F:37:1F:A7:77:78:7B:CD:BD:0A:1C:83:FF

TACAR hosts 23 trust-anchors and provides support to the EUGridPMA (European Grid Policy Management Authority) group. TACAR has been endorsed by the eIRG (e-Infrastructure Reflection Group, a policy definition body sponsored by the EC) together with the EUGridPMA as a significant step to enable collaborative e-science in Europe.

### 3. Campus Middleware Issues

TF-EMC2 also aims to encourage the use of middleware technologies in campuses.

Enabling the campuses to understand the end-users needs is in fact one of the main strategic goals of the Task Force. With respect to this, work so far concentrated on the organisation of events to train and provide hands-on experiences to IT practitioners in the European academic institutions (inspired by Internet2 CAMP).

The first of these events, called **EuroCAMP** (European Campus Middleware Planning) was held in March 2005, in Turin (Italy) and organised by TERENA. EuroCAMP was a three-day workshop, which focused on Identity Management Systems and federated access both to applications and the network itself.

The event targeted Internet Technology architects and technical managers of universities and research centres and representatives of national research and education networks in Europe who are involved in designing campus-wide digital identification (ID) systems, and for others involved with digital ID systems in academia.

Considering the success of the first EuroCAMP, TERENA has decided to organise two EuroCAMP per year (spring and fall periods), with the idea that one of the two events will introduce new topics of interest.

The next **EuroCAMP** will take place in **November (7-9) 2005 in Porto** (Portugal).

More information about EuroCAMP is on line at: <http://www.terena.nl/tech/>

## 4. Directory schema

(<http://www.terena.nl/tech/task-forces/tf-emc2/dir.html>)

The need of interoperability among different components has increased awareness on the role that attributes play. Information is stored as schemas; each schema is a collection of attributes definitions, where attributes describe the characteristics of the object that the schema is meant to represent.

Interoperability among different software translates into schema and attributes exchange and the coordination of schemas is a real need to foster collaboration. In different contexts (or to say schemas used in different countries) the same attributes can mean different things, not to mention that different regulations deal with privacy issues related to attributes in different ways.

**SCHAC**, which stands for SSchema HARmonisation Committee, is a dedicated working group that operates (since February 2005) within TF-EMC2 with the aim of defining and promoting common schemas in the field of higher education under the aspect of inter-institutional data exchange. To date eduPerson represents the only successful attempt in this area, but it is mainly tailored to American needs.

Members of institutions will not be requested to give up their internal schemas, but they will be requested to use the SCHAC schema for (inter)national data exchange.

SCHAC hopes to provide support for the JRA5-AAI activities (for Eduroam as well) and in for Grids and activities related to the deployment of federations. EUNIS is also interested in using the SCHAC schema for the ECTS (European Credit Transfer and Accumulation System) project.

Different national schemas (Poland, Spain, Norway/Sweden, etc) have been evaluated in the beginning to search for commonalities. Two releases of the SCHAC attributes for personal data have been produced so far, both available on line.

(<http://www.terena.nl/tech/task-forces/tf-emc2/schac.html>)

# TERENA Middleware Activity Report

## 5. Other TF-EMC2 activities

### SCS - Server Certificate Service

<http://www.terena.nl/tech/task-forces/tf-emc2/scs.html>

TERENA through TF-EMC2 provides also support for small projects in the middleware area, whenever there is a sufficient interest among the of task force members.

An example of this is the project, known as **SCS (Server Certificate Service)** to acquire a Certification Authority (CA) service from a commercial CA to allow NRENs or national organisations representing the academic community to get as many server certificates they need by paying a yearly amount. This project aims to solve the so-called 'pop-up' problem, which arises when using server certificates issued by a CA whose root is not listed among those recognised as trusted by web browsers.

The preliminary analysis about the feasibility of the project has been conducted and the procurement to acquire the service started in August 2005.

TERENA has prepared a Call for Proposals, which has been published on the project page (<http://www.terena.nl/tech/task-forces/tf-emc2/scs.html>) as well as in the Official Journal of the European Commission.

The deadline to submit a proposal is September 30<sup>th</sup> 2005. After this deadline the most suitable proposal will be selected among the one received and a contract will be signed, in order to start the service in November 2005.

### Dissemination support

One of the most important roles that TF-EMC2 performs is to provide a middleware discussion forum for the academic community in Europe and beyond.

In order to avoid duplication of work and to assure that the results achieved by the group are compliant with the standards followed by the scientific community, TF-EMC2 liaises with international middleware groups and standardization bodies.

The task force has been able to attract people working in the Grid arena, providing the NRENs and the Grid community with an opportunity to exchange information about the technologies in use in the two different environments.

# TERENA Middleware Activity Report

This liaison has generated some discussion about the way PKI is used and implemented in Grid applications, which was concluded with the production of a document to highlight differences and/or analogies of Grid-PKIs versus NREN-PKIs.

The document is available on line under the topic at:

<http://www.terena.nl/tech/task-forces/tf-emc2/international.html>

In December 2004 a small survey was conducted among the TF-EMC2 members with the aim of gathering information about the AA developments and to make them available on a single web page.

(<http://www.terena.nl/tech/task-forces/tf-emc2/aai.html>).

The idea behind this is to provide as much information as possible about the state of the art and make it available to anybody visiting the TF-EMC2 web site. The information collected is updated regularly. A PAPI-based wiki will be used in the future to allow for easier maintenance.

## TF-EMC2 Future

TF-EMC2's mandate expires in September 2006.

The Task Force has consolidated its position as a *neutral point* for information exchange and consensus growing among NRENs (not only in Europe, but in Australia and the USA) and other communities, like the Grids. Middleware is essentially about interconnecting different elements and standards. An important growth of the role played by EMC2 in these processes is foreseeable in the short and mid term. This role is not only limited to a forum itself, but also to the possibility of evaluating, developing and acting as focal point for the diffusion of new technologies and ideas.

The activity on building awareness about middleware technologies among the constituencies of the different NRENs is also vitally important. This activity, started with the EuroCAMP, offers a two-way communication channel: from NRENs and international communities to user institutions, making them aware of new technologies and standards, and from user institutions to NRENs, making them aware of needs and internal developments.

# TERENA Middleware Activity Report

New topics might cover Virtual Organisations issues and federations, due to the increasing interest of these technologies. A new area to explore is also the one related to inter-federations issues, mainly at technical level.

Diagnostic is a potential area of interest as well, mainly for what concerned the standardisation of log files.

## TF-Mobility: history, status and future

[\(http://www.terena.nl/tech/task-forces/tf-mobility/\)](http://www.terena.nl/tech/task-forces/tf-mobility/)

### Introduction

The TERENA Task Force Mobility was established at the beginning of 2002. The task force, which ran for an initial one and half year period, had a well defined focus, namely the definition and testing of an inter-NREN roaming architecture, based on standard technologies selected among those used by the NRENs involved in the task force.

A RADIUS backend approach between a number of NRENs and SURFnet using a Radiator RADIUS proxy server hierarchy was successfully developed and different network access methods (802.1X and Web-based redirection) over the RADIUS proxy hierarchy tested. Also a proposal for VPN-based solution was developed.

The pilot service resulting from these tests is known as eduroam: the educational roaming infrastructure based on 802.1X standard technology and RADIUS proxy servers backend to provide access to a visited wireless network.

In June 2004, during the TERENA Conference, eduroam was available for the eduroam participants.

### TF-Mobility aims and relationship with GEANT2-JRA5

In September 2004 a proposed new version of the charter for the next 2-year period of TF-Mobility was approved by TERENA. The task force is co-chaired by: Klaas Wierenga (SURFnet) and David Simonsen (UNI-C).

TF-Mobility, together with TF-EMC2, is one of the TERENA Task Forces that liaise closely with one of the GEANT2 JRA5 (focused on Aunthorisation and Roaming).

At the time JRA5 started eduroam was already quite used in the academic community therefore it was agreed to use eduroam as the base for the JRA5 roaming infrastructure, enhancing it into a full service. Some of the countries see already their national eduroam infrastructure as a production service level, but this is not universally true.

# TERENA Middleware Activity Report

A number of technical and policy enhancements are needed and are currently taking place in the framework of the JRA5 project.

Whereas JRA5 is focused on the enhancement of the technical elements that are part of eduroam and its ultimate goal is to upscale eduroam to a full service, TF-Mobility focuses on the exploration of new roaming technologies especially those not covered by JRA5. TF-Mobility, through the dissemination activity, also connects new members to eduroam and provides technical support for them to join.

The TF-Mobility group also provides a forum to discuss the findings of JRA5 with international partners like Internet2 and the Asia-Pacific region and other non JRA5-participants.

The technical discussion that takes place on the TF-Mobility mailing list tackles eduroam operational issues and allows technical experts to report on their experiences.

The working items that are the focus of the TF-Mobility are the following:

1. Mobility Next Generation
2. End Users Mobility
3. Managing Monitoring
4. Deployment Issues

## 1. Mobility Next Generation

<http://www.terena.nl/tech/task-forces/tf-mobility/nextgeneration.html>

This task focuses on the use of new technologies to provide the authentication and authorisation functions for eduroam (currently provided by the RADIUS) as well as on operational issues.

The person responsible for this task is Miroslav Milinovic (CARNET).

At the moment eduroam provides three different functionalities:

- **authentication of the users:** the institution part of the username of the type `user@institutions_name.country`, also called realm, is used to find the user home institution authentication server, which in the current implementation is a static routing map. Some investigations are being carried out to make this process more dynamic. The use of DNSSec, DIAMETER etc is being investigated.
- **a protocol to transport users' credentials** to the users home institution: the authentication is currently carried over the RADIUS infrastructure. The possibility to

# TERENA Middleware Activity Report

provide direct ad-hoc connection from a guest network to the home users' AA server is being investigated through the use of RADIUS over IPsec and DIAMETER.

- **a trust fabric:** Current trust fabric is implemented as a chain of peer-to-peer shared secrets between RADIUS servers. Some studies to use PKI to enhance the system are being performed.

In the operational field, to increase redundancy of the eduroam infrastructure an extra Top Level RADIUS Proxy Server (TLRPS<sup>2</sup>), to work together with the one managed by SURFnet (the Netherlands) is maintained by UNI-C (Denmark).

CARNET has produced an XML schema to display the status of the various RADIUS servers in an HTML page.

A useful discussion about the use of various SSIDs for eduroam took place on the TF-Mobility mailing list; the result of such a discussion was a **guideline document** (produced by Tomasz Wolniewicz from the Polish Nicolaus Copernicus University). The document was circulated over the list in July and will be reviewed during the meeting in September (2005).

## 2. End Users Mobility

<http://www.terena.nl/tech/task-forces/tf-mobility/endusers.html>

This area focuses on the use of tools to make it easier for end users to connect to an eduroam enabled wireless LAN.

The person responsible for this area is Klaas Wierenga (SURFnet).

The tasks undertaken in this area are:

- **eduroam web site maintenance:** Licia Florio (TERENA) is responsible for maintaining the information on the eduroam web site (<http://www.eduroam.org>). The web site provides information about all the eduroam developments and the countries that are connect. To-date more than 18 countries in Europe are connected to eduroam; Australia was the first non-EU country to connect (December 2004). Since May 2005 eduroam (both the name and the logo) has been registered as a TERENA trademark.

---

<sup>2</sup> The servers are also called European Top Level RADIUS Server (ETLR).

# TERENA Middleware Activity Report

- **iPass Solution for NRENs:** iPass is commercial software that through a client installed on the users machine, gives Internet access for travelling users in about 150 countries via local phone calls, WiFi or wired Ethernet. Users need to be authenticated for security and usage billing purposes.

UNI-C has signed a one year contract for the Danish academic institutions with iPass. This is to be extended to include a number of other European NRENs on the assumption that there will be an interest for this kind of service.

Each NREN subscribing to the service gets a set of clients for PC, Mac and PDA with the NREN logo for download by the NREN's customers. The NREN also gets a realm (basically a domain name) assigned and each customer will get an unique username.

Travelling users can connect to a local iPass partner ISP who sends username, realm and password via encrypted channels to these roam servers.

The NREN's user administration is operated by a username and password database located at UNI-C. UNIC has developed software with web interfaces which will allow the NREN and its assigned customer universities and their assigned departments to manage the user database, and users to manage their own password and data. Each NREN will also get call data records (CDR) for their users' traffic for administration and billing.

UNI-C has also tested the integration of iPass with eduroam to provide connectivity to the users in places not covered by eduroam.

A **deliverable** to report the results and the recommendations about the use of iPass in combination with eduroam will be ready in September 2005.
- **Access point phone book:** to help users discover where eduroam is available, SURFnet has proposed to use a database containing location information about eduroam Access Points. A first draft of the database structure was circulated to the list in January 2005. Compliance with the commercial operators' database model is being investigated. Issues to be finalised in order to use the database are the fields used to store the data, the way to populate the database and the way to keep it up-to-date.
- **Eduroam client:** One of the possible ways to overcome the diversities of SSIDs and ciphers is to have a client that makes these details transparent to the users. The group is currently investigating a way to produce the so called 'eduroam client'.

# TERENA Middleware Activity Report

## 3. Managing and Monitoring of Use and Abuse

<http://www.terena.nl/tech/task-forces/tf-mobility/monitoring.html>

This working area focuses on the monitoring of the eduroam infrastructure in particular the RADIUS servers.

The person responsible for this task is Josh Howlett (University of Bristol, UK).

The following tasks are being undertaken in this area:

1. **RADIUS Monitoring:** this task looks into the RADIUS servers availability, the way the authentication is performed over the RADIUS infrastructure and the end-2-end monitoring.
2. **RADIUS Management:** the aim of this task is to provide some guidelines about the configuration as well as accounting guidelines.

The work in this area is still progressing; most of the information is available on the wiki server (<http://www.eduroam.org/wiki/ManagingMonitoring>)

## 4. Deployment Issues

<http://www.terena.nl/tech/task-forces/tf-mobility/deployment.html>

In order to support users and allow also small institutions to participate in eduroam without making big investments, the group explored the possibility to install in one box all the necessary software to operate a fully functional integrated Web, VPN, 802.1X access point (AP). It was agreed that eduroam-in-a-box would demonstrate the benefits of eduroam and would lead most sites to be able to present a case to fund modifications to their existing access points to be eduroam enabled. It was also confirmed that ideally, eduroam-in-a-box would be capable of supporting a lightweight RADIUS solution and authentication database.

The task, which was carried out initially by Hansruedi Born (SWITCH) and then by Ralf Paffrath (DFN) has been completed and the new version of the product is available at:

<http://www.dfn.de/content/dienstleistungen/dfnroaming/knoppix/download/>  
[agreement/](#)

The new version has a configuration script that allows for the use either only the VPN/WEB solution (in case no 802.1X capable access points is available) or all three sorts of authentication methods as desired and in case SSID/VLAN support on the access point side is available.

# TERENA Middleware Activity Report

A **deliverable** to detail how to use the all-in-a-box solution is under preparation and will be ready in September 2005.

## TF-Mobility Future

Eduroam is widely regarded as a highly successful project and many users rely upon its services.

In September 2006 the group will have to decide which path to take, whether to focus the efforts on a single topic of general interest or broaden up to become a general mobility forum.

Mobility is clearly an area of interest for the TERENA community and the emerging of new technologies allows for quick developments, which provide a lot of inputs for discussions and ideas for new possible projects.

## Appendix

This appendix contains the list of the meetings held by the task forces in the last year. Minutes of the meetings are available on the related web pages.

### TF-EMC2 Meetings

TF-EMC2 met three times since the starting of its mandate.

The *first meeting* was held in November 2004 to refine the charter and agree a roadmap for the work to be carried out.

The *second meeting*, held in February 2005, was focused on the technical work items as well as in agreements of deadlines for the coming months.

Discussions about ideas for possible new projects took also place (most of these ideas are still being discussed by the group).

The *third meeting* took place in Poznan (June 2005), during the TERENA Conference and due to high number of events, it was possible to organise only half day meeting. The meeting provided an opportunity for the attendees to report about the results achieved in the various working items.

A two-day meeting is scheduled in September (8-9) 2005 in Barcelona. To facilitate discussion and to maximise the time, this meeting will be take place in conjunction with JRA5 and TF-Mobility.

### TF-Mobility Meetings

The *first taskforce meeting* took place in Berlin (September 2004), when the charter was reviewed and specific work items and the scope of work was agreed. Owners and participants were assigned to work items and discussions on priorities and timescales finalised.

The *second meeting* was held via videoconference. This meeting focused on progress updates from the various deliverable owners with discussions on the work plans as well as general discussions on current eduroam issues.

The *third meeting* was held in Zurich (January 2005). This meeting utilised the eduroam wiki to update progress based on owner's updates, there were many lively discussions. Eduroam access was made available over web-based redirect and 802.1X courtesy of DFN (German NREN).

# TERENA Middleware Activity Report

The *forth time* the task force met in Poznan (June 2005), for a half day meeting. Due to the limited time, the meeting was used to review the list of deliverables and for a short update from the group.

A one-day meeting has scheduled on the 6<sup>th</sup> of September 2005, the day before JRA5 meeting.