13.07.10

Deliverable DS3.1.1: Report on the Establishment and enhancement of the Policy Management Authority and Repository

Deliverable DS3.1.1

Contractual Date:	31/05/10
Actual Date:	13/07/10
Contract Number:	238875
Activity:	SA3
Work Item:	T1
Nature of Deliverable:	R (Report)
Dissemination Level	PU (Public)
Lead Partner	TERENA
Document Code	GN3-10-157
Authors:	L. Florio (TERENA), W. Singer (DANTE)

Abstract

This document reports on the work undertaken to establish and enhance the Policy Management Authority (PMA) and TACAR Repository, and the results achieved by the eduPKI Task (SA 3 Task 1). It describes the enhancement to the existing TACAR software, the governance of the PMA and related procedures, and the Certification Authority (called eduPKI CA) developed by the eduPKI Task. It also describes the eduPKI PMA assessment of the eduroam service's requirements concerning digital certificates and the solution proposed and tested for this specific case.

Table of Contents

Table of Figures

0 Executive Summary

eduPKI aims to ease the usage of digital certificates for GÉANT services, offering the necessary expertise and facilities to support them in a cost-effective manner. The eduPKI work carried out during Year 1 of the project focused on three main areas:

- Defining the governance of the eduPKI service.
- Enhancing the existing TERENA Academic CA Repository service (TACAR), which will be used as a support repository for the eduPKI work.
- Setting up a Certification Authority (eduPKI CA) to demonstrate how the eduPKI service would work.

Work on the areas listed above has progressed on schedule and, by end of April 2010, the enhanced version of TACAR and the prototype of the eduPKI CA were delivered.

At the beginning of 2010, the eduPKI Policy Management Authority (PMA) worked closely with the Joint Research Activity 3 (JRA3) Task 1 (Roaming Developments) to support the new eduroam architecture (eduroam next-generation) under development in JRA3 Task 1. eduPKI's support for eduroam is aimed at developing the mutual authentication and authorisation of RADIUS (Remote Authentication Dial In User Service) nodes within the eduroam infrastructure. The eduPKI solution, devised by the eduPKI task to support eduroam next-generation requirements, proposes ways of encoding the eduroam node properties into a digital certificate.

Once the test phase is completed, which is expected by September 2010, plans are in place to deploy these certificates in eduroam.

This document reports on the work undertaken to establish and enhance the PMA and TACAR Repository, and the results achieved by the eduPKI Task (GÉANT Service Activity 3, Task 1), which is responsible for this work. It describes the enhancement to the existing TACAR software, the governance of the PMA and related procedures, and the Certification Authority (called eduPKI CA) developed by the eduPKI task. It also describes the eduPKI PMA assessment of the eduroam service's requirements concerning digital certificates and the solution proposed and tested for this specific use-case.

1 Introduction

Service Activity 3 (SA3) Task 1 of the GÉANT (GN3) project is known as eduPKI. The objective of eduPKI is to facilitate access to, and the use of, Public Key Infrastructure (PKI). Public key infrastructure is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates; see [PKI].

Many services already make use of X.509 certificates issued by Certification Authorities (CAs) operating PKIs. It is anticipated that the demand for CA-issued certificates will increase in the coming years due to a growing requirement for secure communications. To meet this demand, and to permit the use of existing national PKIs (in most cases operated by NRENs) for GÉANT services, there exists a requirement for some coordination of the work and a limited central service.

eduPKI aims to offer the necessary support and expertise to other GÉANT services to enable them to use digital certificates. The benefits of this work include:

- Promotes the adoption of digital certificates (both personal identity certificates and server certificates) within the project in a cost-effective way.
- Enables GÉANT services to use existing PKIs (usually operated by NRENs) that meet their requirements.
- Allows users of GÉANT services to obtain all necessary certificates from a single CA (normally the one operated by their own NREN). A new centrally operated PKI will issue certificates to users whose NREN does not operate a suitable CA.
- Improves coordination to address security requirements of the services being developed in the project and will create a service able to support other services in defining their security requirements.

eduPKI services

To achieve the objectives described above, eduPKI offers three main services:

- **The Policy Management Authority (PMA)**, which defines the governance procedures for the eduPKI service.
- **An enhanced version of the existing TACAR system**, operated by TERENA (TERENA Academic Certificate Authority Repository), used to store and distribute the eduPKI-participating Certificate Authority's root certificates (including the eduPKI CA root) in a secure manner. See [TACAR]
- **A dedicated Certification Authority (eduPKI CA)**, operated by DFN for test purposes and to support those NREN users that cannot rely on any national CA (CA used by the NREN, including both commercial and non-commercial) service.

The relationship between these services is illustrated in Figure 1 below.

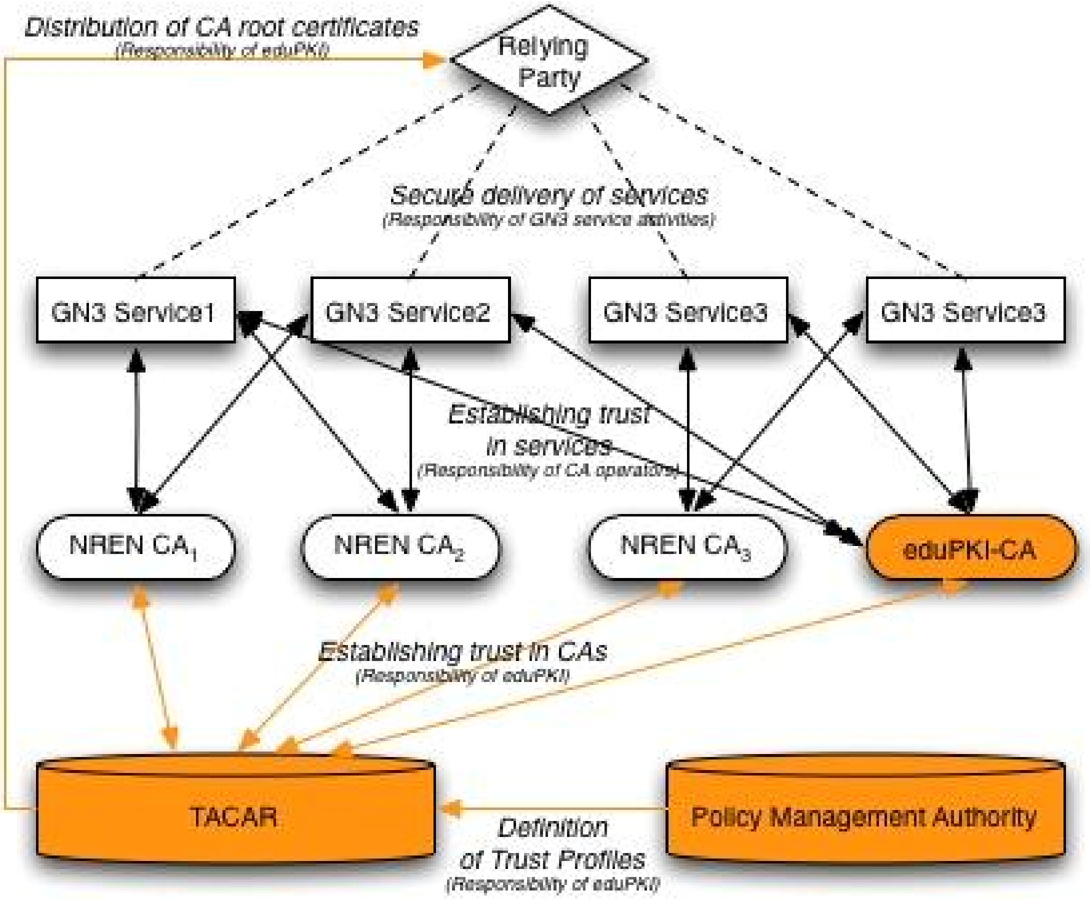

Distribution of CA root certificates
(Responsibility of eduPKI)
Relying Party
Secure delivery of services
(Responsibility of GN3 service activities)
GN3 Service1
GN3 Service2
GN3 Service3
GN3 Service3
Establishing trust in services
(Responsibility of CA operators)
NREN CA1
NREN CA2
NREN CA3
eduPKI-CA
Establishing trust in CAs
(Responsibility of eduPKI)
TACAR
Policy Management Authority
Definition of Trust Profiles
(Responsibility of eduPKI)

Figure 1: Role of TACAR, PMA and eduPKI CA in the distribution of digital certificates

The elements (services) in orange in the Figure 1 above are under direct eduPKI responsibility. The PMA defines **Trust Profiles** (a minimum set of trust requirements for a CA; for details see Section 2); the PMA will create Trust Profiles based on the services' requirements. If an existing profile matches the requirements of the service, the service will be encouraged to use this profile. If there is no suitable profile, a new profile will be created for the service.

TACAR will contain categories mapping the Trust Profiles. NREN CAs that wish to issue certificates in accordance with these Trust Profiles will request the PMA to accredit them against the Trust Profiles. TACAR will show which NREN CAs have been accredited and under which profile.

If an NREN CA is accredited according to a specific profile, this NREN CA will then be in a position to issue certificates for the specific GÉANT service for which the profile has been designed. The trust between the service and an NREN CA is then established: the service and NREN CA trust each other because the eduPKI has accredited that NREN CA (for this reason a black arrow is used).

Lastly, the user will interact with the certificates issued by NREN CAs directly or indirectly: directly when the user obtains a personal certificate issued by one of the accredited CAs; indirectly whenever the user can successfully use a GÉANT service (for instance, most of the services require TLS connections between clients and servers).

For more information on eduPKI, see Appendix A.

eduPKI sub-tasks

eduPKI (SA3-T1) has been broken down into the following sub-tasks:

- Defining procedures for the eduPKI PMA and the governance for the eduPKI services.
- Enhancing the features of the existing TACAR repositories.
- Providing a proof-of-concept of the proposed Certification Authority (eduPKI CA) for test and a support purposes.
- Addressing the first use-case for eduPKI: based on the results of the services' evaluation (performed in 2009 and detailed in the eduPKI status report [eduPKI]) eduroam was selected as the first service eduPKI will support.

Achievements during Year 1

Table 1-1 below summarises the achievements of eduPKI during Year 1.

Achievement	Description
Enhancements to the PMA	The PMA's procedures are now documented in the "PMA Charter". The initial version of this document was completed in February 2010.
Enhancements to TACAR	The TACAR repository has been enhanced to include a new "category" management feature. Category management will enable the eduPKI PMA to manage the categorisation of the specific certificate profiles that are being designed for the GN3 services. TACAR's user interface was also improved, allowing easier management of the TACAR content. The new software was released at the end of March 2010.
eduPKI CA proof of concept	The Task established an eduPKI CA that was initially used for testing purposes by the group and by the participating GN3 services. The CA became available in April 2010.
First use-case for eduPKI	eduroam was selected as the first service that eduPKI will support.

Table 1-1: eduPKI Achievements during Year 1

The remainder of this document reports on the progresses in each of the areas listed above.

2 Enhancements to the eduPKI PMA

The eduPKI Policy Management Authority (PMA) is the centrepiece of eduPKI. Established at an early stage in the GN3 project (M3), it consists of a group of technical experts within the GN3 project who evaluate CAs that issue X.509 digital certificates for the GÉANT community. The eduPKI PMA defines and maintains the minimum set of criteria that must be met by participating CAs, and accredits candidate CAs on the basis of an evaluation of their policies against these criteria.

The eduPKI PMA also establishes connections and mediates between Certification Authorities (CAs), Relying Parties, Trust Profiles and the Trust Anchor Repository (TACAR):

- **Certification Authority (CAs)**: infrastructure (hardware, software and policy) used to issue a certificate binding a public key to an identity or a DNS-entry.
- **Relying Party**: an entity that relies on the electronic identity credential and trusts the process followed to ensure that the identity represents the individual named in the credentials.
- **Trust Profile**: indicates the minimum requirements that a CA must fulfill to meet the demands of a service.
- **Trust Anchor Repository (TACAR)**: TERENA Academic CA Repository. A trusted repository which contains verified root-CA certificates.

For details, see Section 2.3.2 and Section 2.3.4.

2.1 PMA membership and structure

A PMA member is an expert that works for the PMA, performing one of the tasks of the PMA.

The PMA currently has two members: Milan Sova (CESNET) and Reimer Karlsen-Masur (DFN-CERT Services GmbH). PMA members are appointed by the eduPKI PMA, based on the expertise of individual candidates. GÉANT management team appoints one person[1] (plus a back-up for this role) to follow the operations of the eduPKI PMA. It is foreseeable that this will expand in the future to include more members.

It is not planned for accredited CAs to automatically become members of the PMA, although experts from CAs/NRENs can become members if they are prepared to assume some of the workload of the PMA. Certain

[1] Otto Kreiter from DANTE has been nominated for this role.

roles may be needed in the long term (e.g. a chair) to formally establish and operate the PMA. Figure 2 below illustrates the structure of the PMA.

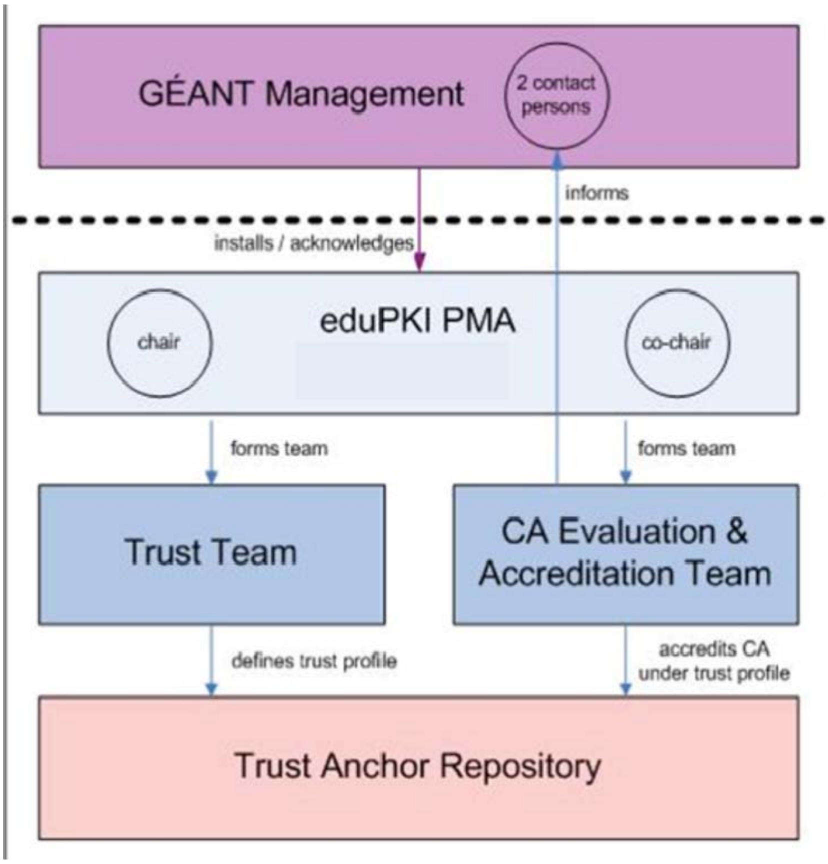


Figure 2: eduPKI PMA Structure

Figure 2 above shows the eduPKI PMA (installed by GÉANT management), PMA Tasks and the relation to the TACAR Trust Anchor Repository. If the PMA grows, two teams — a Trust team, and a CA evaluation and accreditation team — could be defined to take responsibility for the main tasks of the PMA.

2.2 PMA Responsibilities

The PMA is responsible for the following main tasks:

- Assessing GÉANT services' requirements and existing NREN-operated CAs' policies against GÉANT services' requirements.
- Defining **Trust Profiles**, which will indicate the minimum requirements that a CA must fulfill to meet the demands of a service. This may include, for example, the necessary procedures for authenticating the identity of a person (e.g. by email, postal address or in person using an official identity document) or to verify the ownership of a DNS domain. For more information on the Trust Profile, see Section 2.3.4.

- Defining an **Accreditation Procedure** that will describe how new CAs are evaluated against the profiles. It will also describe an escalation process in case of disagreement.
- Defining procedures to indicate how NREN CAs should be stored and maintained into the repository (TACAR).

2.3 PMA Documents

SA3-T1 develops governing documents and procedures for the work of the PMA. The procedures are defined in the following three governing documents and in an additional set of Trust Profile documents:

- eduPKI Charter document
- eduPKI PMA GÉANT Services Registration Process document
- eduPKI PMA CA Accreditation Process document
- set of eduPKI Trust Profile document

Each of these documents is described briefly below.

2.3.1 The eduPKI PMA Charter

The eduPKI PMA Charter document is the foundation of the PMA. It describes how the PMA is set up and operated, its scope, objectives and responsibilities, membership and voting processes.

The first version of this document was completed in February 2010 and has been approved by SA3-T1 and published internally on the GÉANT intranet; the document will be published externally shortly. See [eduPKI.

2.3.2 eduPKI PMA GÉANT Services Registration Process

This document describes how a GÉANT Service can register with the eduPKI PMA as a Relying Party under one or more Trust Profiles. (A relying Party is an entity that relies on the electronic identity credential and trusts the process followed to ensure that the identity represents the individual named in the credentials.)

In order to register the service, the Relying Party must either pick the appropriate Trust Profiles, or, if none is available, it must define its own trust requirements and then together with the eduPKI PMA derive an eduPKI PMA Trust Profile. This document also describes how a Trust Profile is defined.

This document has been approved by SA3-T1 and will be published shortly on the GÉANT website.

2.3.3 eduPKI PMA CA Accreditation Process

The eduPKI PMA CA Accreditation Process document describes the process of how a X.509 Certification Authority (CA) can obtain eduPKI PMA accreditation under a specific eduPKI Trust Profile by being reviewed by the eduPKI PMA; it also describes how an accredited CA is securing its accreditation by adopting changes to comply with the relevant eduPKI Trust Profile, performing audits and delivering their audit reports; as well as how accreditation of an accredited CA is withdrawn.

The first version of the eduPKI PMA CA Accreditation Process was delivered at M11; however further refinements were needed and the final version of the document will be made public in July.

2.3.4 Set of eduPKI Trust Profile Documents

The eduPKI PMA collects trust requirements from GÉANT services that wish to deploy or use asserted identities based on X.509 digital certificates issued by a PKI for their authentication needs and – based on these requirements, best practices and standards – defines various sets of minimal criteria to be met and implemented by these PKIs. These sets of minimal criteria, called ***Trust Profiles***, represent the different requirements; trust characteristics and identity assertions that GÉANT services have in regards to their authentication needs.

The structure and outline of an eduPKI Trust Profile is defined by the eduPKI PMA GÉANT Services Registration Process document. The eduPKI team is developing the first eduPKI Trust Profile (the eduroam profile), based on the eduroam requirements. More details on the development of the eduroam profile are provided in Section 5.

The Trust profile documents are currently being drafted and will be published on the GÉANT website. Work for the eduPKI Trust Profile for eduroam is described in Section 5.

3 Enhancements to the TACAR Repository

The TERENA Academic Certification Authority Repository (TACAR) is used by eduPKI (SA3-T1) as the solution for provision of a trusted repository which can contain verified root-CA certificates.

In Year 1 the TACAR repository was enhanced to include a new “category” management feature. Category management will enable the eduPKI PMA to manage the categorisation of the specific certificate profiles that are being designed for the GN3 services. TACAR’s user interface was also improved, allowing easier management of the TACAR content. The new software was released at the end of March 2010.

Section 3.1 below provides an overview of the use of the TACAR repository, and Section 3.2 provides details of the enhancements to the Repository in Year 1 of the project.

3.1 Overview

The majority of CAs operated by the NRENs are not pre-installed on operating systems or applications. For these CAs it is necessary to import their root certificates into the operating system or applications to enable the verification of certificates that purport to come from these CAs.

TACAR was launched by TERENA in 2003 to demonstrate the feasibility of using a trusted repository for gathering and distributing root-CA certificates not pre-installed into operating systems or applications. From 2005 TACAR grew significantly, serving as a single source for all relying parties to validate their trust infrastructure for the IGTF (International Grid Trust Federation) and for many other academic identity providers. Today TACAR hosts about 50 root-CA certificates operated for research and education purposes worldwide.

During the preparation of eduPKI workplan, the need became evident for a repository to handle different certificate profiles and to list CAs and the profiles they comply with. It appeared natural to expand TACAR functionality to also support eduPKI needs; in this way TACAR becomes a cross-activity (Grid and GÉANT) trusted repository.

The TACAR policy, online on at: http://www.tacar.org, defines the procedures for gathering and verifying academic root-CA certificates, publishing them in a centralised and trustworthy site and downloading them as an importable trusted file. TACAR users can then download the root CA certificate(s) they are interested in and import it (them) into browsers, mailers or other applications where roots certificates are needed.

It is worth noticing that TACAR **does not** evaluate the policies adopted by the CAs hosted into TACAR or enforce compliance with any particular technical minimum requirements. This has proven to be a strong point for TACAR, as it allows TACAR to work in cooperation with different Policy Management Authorities (PMAs) where policy assessment can be better placed.

TACAR works closely with the International Grid Trust Federation, (IGTF) — see http://www.igtf.org. Most of the root CAs hosted by TACAR to date have undergone IGTF accreditation. TACAR allows displaying those CAs that have been accredited according to the various IGTF profiles. There are currently 40 root CAs hosted in TACAR; none of these are related to GN3.

For more information on TACAR, see Appendix A.

3.2 TACAR Enhancements in Year 1

TERENA has been running a version of TACAR (v1) since 2003. During the preparation of the eduPKI workplan, it was agreed to use a repository to handle different certificate profiles and to list CAs and the profiles they comply with. It was a natural step to expand TACAR functionality to also support eduPKI needs; in this way TACAR becomes a cross-activity (Grid and GÉANT) trusted repository.

The requirements for the new version of TACAR (v2) were collected through interviews with the eduPKI PMA and IGTF members. Based on their answers, it was agreed to review the existing TACAR roles, to reassess what information TACAR should store and to review the workflow.

For a description of roles implemented in TACAR v1, see Appendix A.1. The following roles are implemented in TACAR v2:

TACAR administrators

TACAR administrators are super users with the ability to remove/update all the information contained in the TACAR entries. The TACAR administrator is also in charge of approving the digitally signed email notifications received by the CA representative (CAR).

The TACAR administrator is the only entity enabled to access the TACAR back-end to upload, delete and update the information related to a CA. Access to the TACAR back-end is done using username and password and it requires VPN connection to the TERENA network. To date, only two TERENA employees are able to access the TACAR back-end, to update the current CA information or to add and/or delete root-CA certificates.

Category administrators (CATA)

The CATA is responsible for the management of the various categories (IGTF, GÉANT, others). In the GN3 context, this feature will enable the eduPKI PMA to manage the categorisation of the specific trust profiles that are being designed for the GN3 services. The CATA will log in to TACAR using the federated framework. This feature is not available in TACAR v1.

CA representative (CAR)

The CA representative is the person appointed by the CA to provide all the information related to that CA that should be stored in TACAR.

This role is the same as in TACAR v1; however, the CA representative will be able to upload and/or update the entry he/she is responsible for via the TACAR website rather than by signed email as in v1. The CAR will use the TACAR web interface to upload all the necessary information; once he/she is ready to submit the information to TACAR, the TACAR system will send an email notification to the CAR's email address. At the same time the TACAR system will retain a temporary copy of the information inserted by the CAR.

The CAR has to digitally sign this email and send it to the TACAR administrator. The TACAR administrator will then use the enhanced TACAR back-end to electronically validate the content of the signed email against the information entered by the CAR into TACAR.

If the verification succeeds, the information is permanently entered into TACAR. This process ensures faster response time, maintaining a good security level. This feature is not available in the v1.

TACAR will be used to store root-CA certificates, although the system has been redesigned to allow for storing different types of security tokens, should this feature be needed in the future.

The TACAR roles described above are illustrated in Figure 3 below.

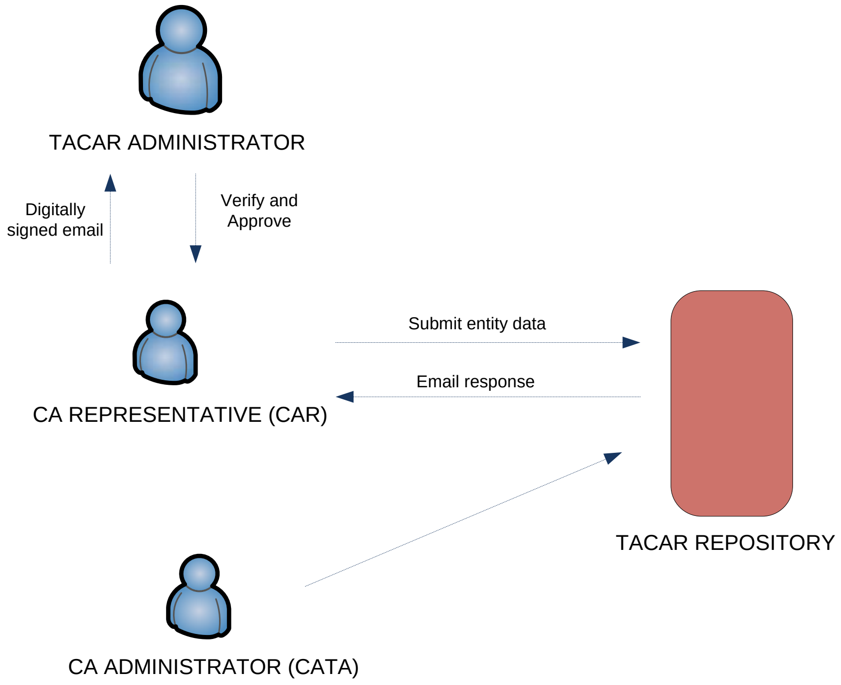


Figure 3: TACAR Users and Roles

3.2.2 Current Status of TACAR

The beta-version of TACAR (v2) was released in March 2010; the software was presented to the IGTF meeting in April 2010 for comments and tests are being performed by the eduPKI PMA. Currently no major issues are reported. The beta version is available at:

https://repos.tacar.org/

Plans are in place to migrate the current content of TACAR to the new system and launch it in July 2010.

For more information on TACAR, see Appendix A.

4 eduPKI CA

SA3-T1 is responsible for setting up and operating the eduPKI CA. The eduPKI CA is a Certification Authority that issues X.509 digital certificates to participants of GÉANT Services who are not able to obtain suitable certificates for these services from a CA local to them. The certificates are issued in accordance with the Trust Profiles defined by eduPKI PMA to meet the demands of GÉANT Services. The eduPKI CA will also be used for testing new Trust Profiles before these profiles are made available to the NREN community.

4.1 Status of the eduPKI CA

The CA became available in April 2010. Currently a proof-of-concept version of the eduPKI CA (eduPKI-test-CA) is being operated by DFN (Germany's NREN). This CA operates for testing:

- The Root-CA certificate
- The issued Certificate Revocation Lists (CRLs)
- The CA's web interfaces
  - for applicants requesting a certificate
  - for applicants requesting the revocation of a certificate
  - for Registration Authority (RA) operators handling and approving the certification and revocation requests
- The certificate profiles as derived from the eduPKI Trust Profiles

Once development of the Certification Policy (CP) and Certification Practice Statement (CPS) for the eduPKI-CA is completed and a production Root CA certificate has been generated, the service will migrate to a production environment and enter the formal accreditation process for selected eduPKI Trust Profiles as defined by the eduPKI PMA.

Plans are in place to migrate the eduPKI CA into production in January 2011.

For examples of the eduPKI web-based User interface, see Appendix A.3.

5 eduroam Use Case

SA3-T1 provides support to other GÉANT services. eduroam [eduroam] is a service with clear requirements for SA3-T1 support and this was the only service with use cases in Year 1.

As result of the first round of interviews with the GN3 services that took place in 2009, a more in-depth discussion with the eduroam service group followed. In the eduroam case, the in-depth discussion led to clear requirements, which define the scenario that the eduroam group was aiming at in the short term.

eduPKI support for eduroam is aimed at the mutual authentication and authorisation of RADIUS nodes within the eduroam infrastructure. The authentication of home RADIUS Identity providers (IdPs) to their users' computers is left in the hands of individual eduroam institutions.

In its current setup, inherited from the GN2 project, eduroam uses URNs (Uniform Resource Names) to identify RADIUS nodes as well as their roles (IdP or SP) in eduroam. The URN is presented in the "*subjectAltName*" extension of a certificate of the particular node.

This solution has several drawbacks: the URN encodes several properties of the node in one place (eduroam membership, member institution identification, the role of the node, the realm the IdP is authoritative for) requiring specific parsing routines not available in legacy software. At the same time, the eduroam community has to maintain a registry of URNs of all registered RADIUS nodes.

Since the current eduroam architecture uses a static hierarchy of RADIUS nodes, the usage of PKI tools is not required, as all the trust is preconfigured manually in the tree setup. However based on the proposal under discussion in JRA3-T1 to move from the current static RADIUS hierarchy to a dynamic model that would enable direct peering between eduroam Service Provider and Identity Provider, the PKI-based node authentication and authorisation becomes important.

In cooperation with the eduroam community, eduPKI proposed a different way of encoding the eduroam node properties in a certificate. Two Object Identifiers (OIDs) have been assigned to identify eduroam SPs and eduroam IdPs, to be used as Policy OIDs in the certificate. The respective Certificate Policy documents have been created. The eduPKI PMA has prepared the eduroam Certification Trust Profile describing the requirements on CAs issuing certificates to eduroam nodes.

The "eduroam Trust Profile" document is in it final stage of approval by eduroam service (SA3-T2), JRA3-T1 and eduPKI groups and is expected to be used by September 2010. When approved, the eduroam Trust Profile will be used as the basis for accrediting a CA that wants to issue eduroam certificates. The eduPKI CA is expected to become the first CA to support this Trust Profile and therefore it will be the first CA to be accredited.

Each of the Trust Profiles defined by the eduPKI will be assigned to a category in TACAR. Once accredited, a CA will appear in the list of the CAs belonging to the matching TACAR category.

In the future, we will extend the certificate profiles defined in the eduroam Certification Trust Profile to include SRV records in the certificate, in order to identify IdP realms as soon as their usage is defined by the eduroam service.

6 Conclusions

Significant achievements have been accomplished by eduPKI (SA3-T1) during Year 1 of the project, leading the Task to start pilot operations.

The Task has been on schedule with the development of the PMA processes and documents (such as the PMA charter and Registration process), which were delivered on time. Work has been done to produce an enhanced version of the TACAR repository (v2), which has been completed on time. A prototype for the eduPKI CA has been delivered as promised. In addition, TACAR has started discussions with one of the services, eduroam (JRA3-T1), and a solution for eduroam's requirements has been provided.

The cooperation with JRA3 Task 1 has proven to be very beneficial for both eduPKI and eduroam.

During Year 2, the eduPKI team plans to engage in a similar discussion with the eduGAIN service (SA3-T3). Plans are in place to also engage with the SA2 team, to assess their trust requirements; some initial steps in this direction have already started.

eduPKI plans to migrate the eduPKI CA into production and finalise the remaining governing documents by January 2011.

7 References

[eduPKI]	http://www.geant.net/Services/EndUserApplicationServices/Pages/eduPKI.aspx
[eduroam]	http://www.eduroam.org/
[PKI]	http://en.wikipedia.org/wiki/Public_key_infrastructure
[TACAR]	http://www.tacar.org/

8 Glossary

CA	A Certificate Authority or Certification Authority is an infrastructure (hardware, software and policy) to issues a certificate binding a public key to an identity or a DNS-entry.
CATA	Category administrators (TACAR)
CAR	CA representative (TACAR)
CESNET	Czech Republic NREN
CP	Certification Policy
CPS	Certification Practice Statement
CRLs	Certificate Revocation Lists
DFN	Deutsches Forschungsnetz; Germany's NREN
IdP	Identity Provider
IGTF	international Grid Trust Federation
OID	**An** Object Identifier is a number that uniquely identifies an object on the Internet.. The assignment of OID is handled via the Internet Assigned Numbers Authority (IANA)
PKI	Public Key Infrastructure (PKI) is s a set of hardware, software, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates
RP	A Relying Party is an entity that relies on the electronic identity credential and trusts the process followed to ensure that the identity represents the individual named in the credentials.
SP	Service Provider
SRV Records	Service Record, RFC 2782
TACAR	TERENA Academic CA Repository. A trusted repository which contains verified root-CA certificates.
URIs	Uniform Resource Identifiers.
X.509 standard	ITU-T defined standard for a public key infrastructure (PKI). The standard X.509 specifies, amongst other things, standard formats for public key certificates, certificate revocation lists, attribute certificates.
RADIUS	Remote Authentication Dial In User Service.

Appendix A Supplementary Information

A.1 TACAR Overview

The system is implemented as a web-based repository, which can be viewed at: http://www.tacar.org .

The main usage for TACAR is to allow relying parties to securely connect to a central point to download one of more root CAs; the download supports different formats, such as pem, pkcs7 and zip archive.

In its original version, TACAR (V1) only allows for three types of users and roles: the CA representative, the TACAR representative (also called Trusted Introducer) and the TACAR administrator.

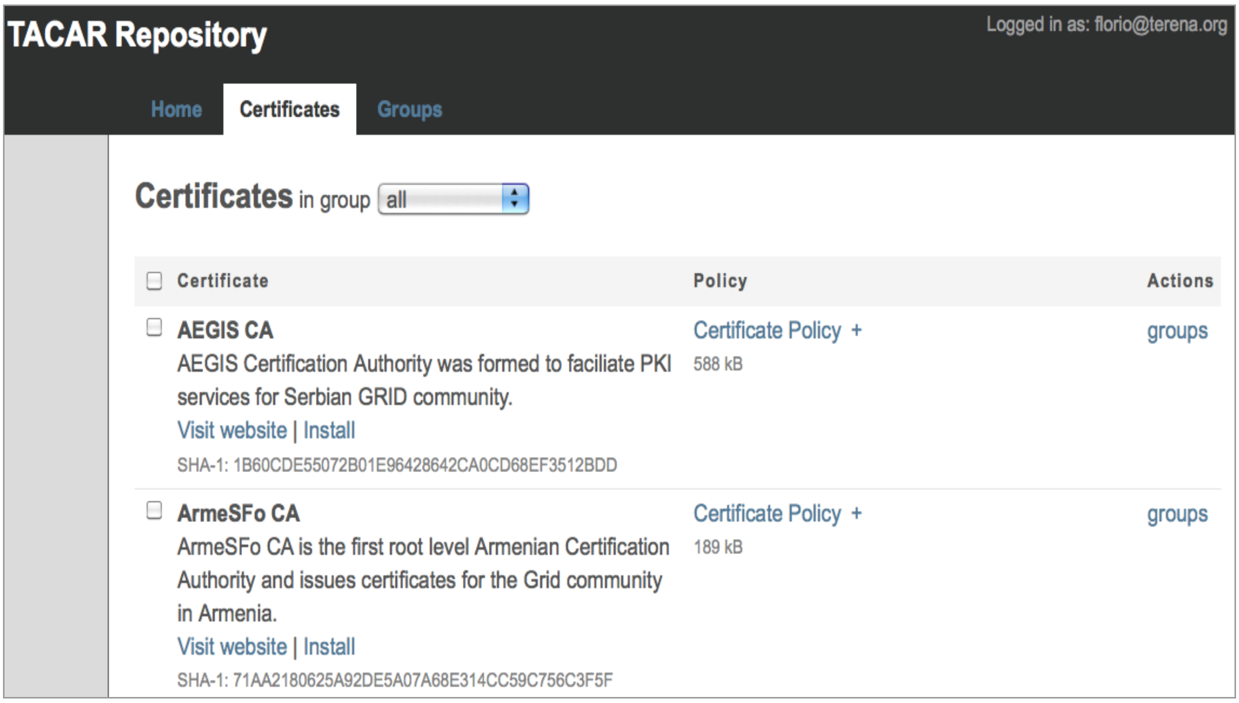
- The **CA representative** is the person appointed by the CA to provide all the information related to that CA that should be stored in TACAR. The first time that a CA applies to enter into TACAR, a signed letter is exchanged between the TACAR representative and the CA representative in a face-to-face meeting. The CA representative does not have rights to access any of the TACAR functionalities. Any update or request for any change has to be dealt with directly by the CA representative and the TACAR administrator.
- The **TACAR representative** is a person delegated by the TACAR administrator to attend the initial face-to-face meeting with the CA representative. After the face-to-face meeting has taken place, the TACAR representative sends the information gathered during the meeting to the TACAR administrator.
- The **TACAR administrator** is the only entity enabled to access the TACAR back-end to upload, delete and update the information related to a CA. Access to the TACAR back-end is done using username and password and it requires VPN connection to the TERENA network. To date, only two TERENA employees are able to access the TACAR back-end, to update the current CA information or to add and/or delete root-CA certificates.

With the growth of TACAR, the current procedure to handle CAs submissions and updates has proven not to be an ideal solution, as it introduced a clear bottleneck, due to the fact that the TACAR administrator needs to be constantly involved in all communications.

The initial TACAR back-end was built in php and uses an SQL database to store the data. Mechanisms are in place to ensure that data is regularly backed up.

A.2 Screen-shots of the TACAR Repository

The figures in this section depict the new TACAR system, developed in cooperation with SA3-T1.



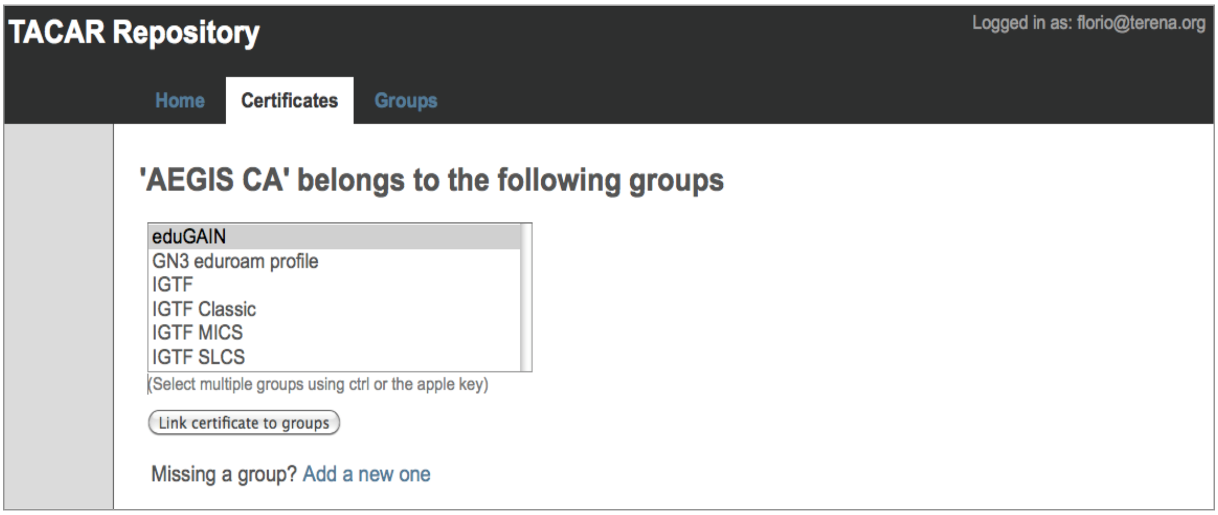
TACAR Repository

Logged in as: florio@terena.org

Certificates in group all

□ Certificate	Policy	Actions
□ **AEGIS CA** AEGIS Certification Authority was formed to faciliate PKI services for Serbian GRID community. Visit website | Install SHA-1: 1B60CDE55072B01E96428642CA0CD68EF3512BDD	Certificate Policy + 588 kB	groups
□ **ArmeSFo CA** ArmeSFo CA is the first root level Armenian Certification Authority and issues certificates for the Grid community in Armenia. Visit website | Install SHA-1: 71AA2180625A92DE5A07A68E314CC59C756C3F5F	Certificate Policy + 189 kB	groups

Figure 4: Example of entities registered in TACAR



TACAR Repository

Logged in as: florio@terena.org

'AEGIS CA' belongs to the following groups

- eduGAIN
- GN3 eduroam profile
- IGTF
- IGTF Classic
- IGTF MICS
- IGTF SLCS

(Select multiple groups using ctrl or the apple key)

Missing a group? Add a new one

Figure 5: Interface to manage categories

A.3 eduPKI Service elements and processes

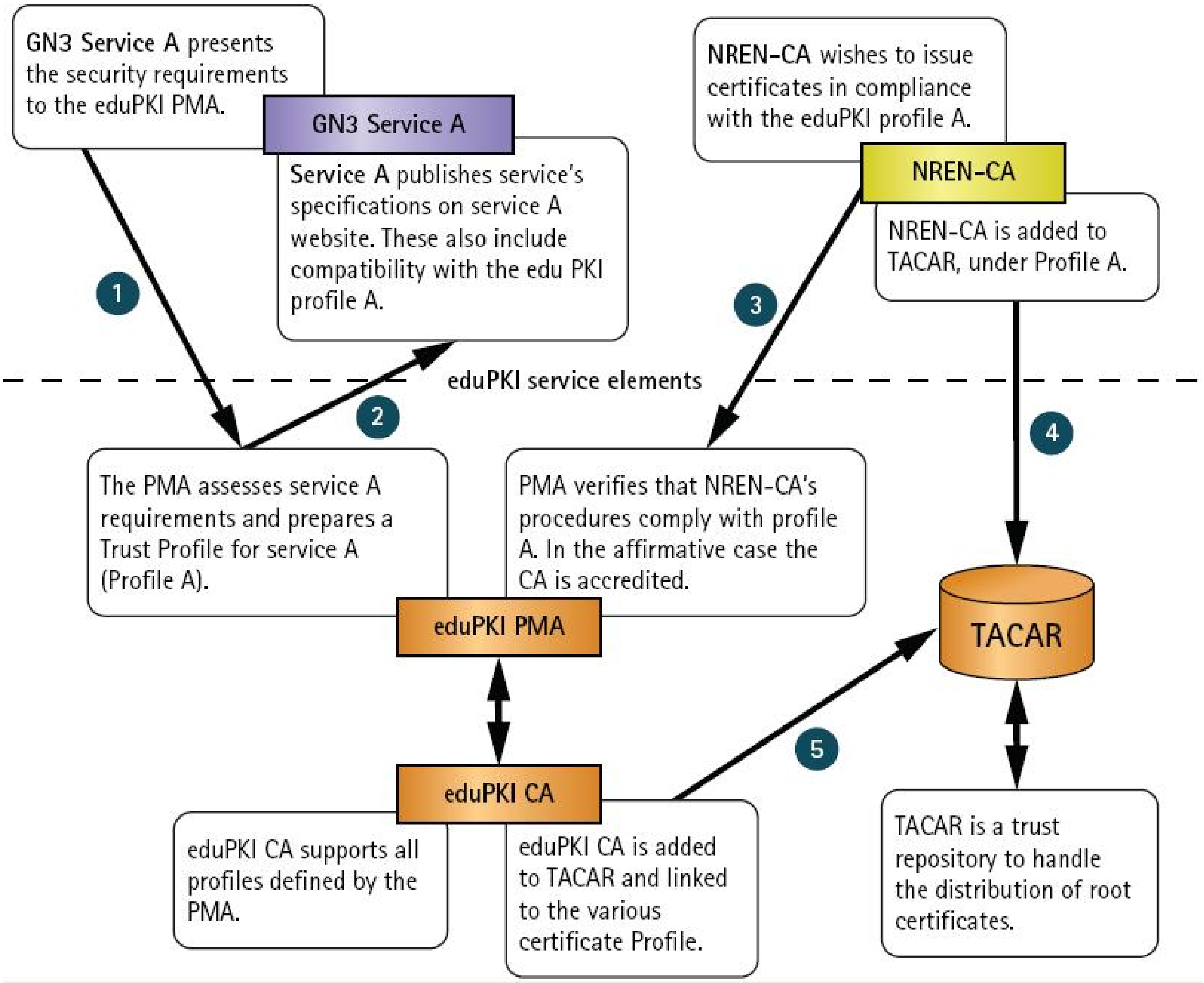

GN3 Service A presents the security requirements to the eduPKI PMA.
GN3 Service A
Service A publishes service's specifications on service A website. These also include compatibility with the edu PKI profile A.
NREN-CA wishes to issue certificates in compliance with the eduPKI profile A.
NREN-CA
NREN-CA is added to TACAR, under Profile A.
1
2
3
4
5
eduPKI service elements
The PMA assesses service A requirements and prepares a Trust Profile for service A (Profile A).
PMA verifies that NREN-CA's procedures comply with profile A. In the affirmative case the CA is accredited.
eduPKI PMA
TACAR
eduPKI CA
eduPKI CA supports all profiles defined by the PMA.
eduPKI CA is added to TACAR and linked to the various certificate Profile.
TACAR is a trust repository to handle the distribution of root certificates.

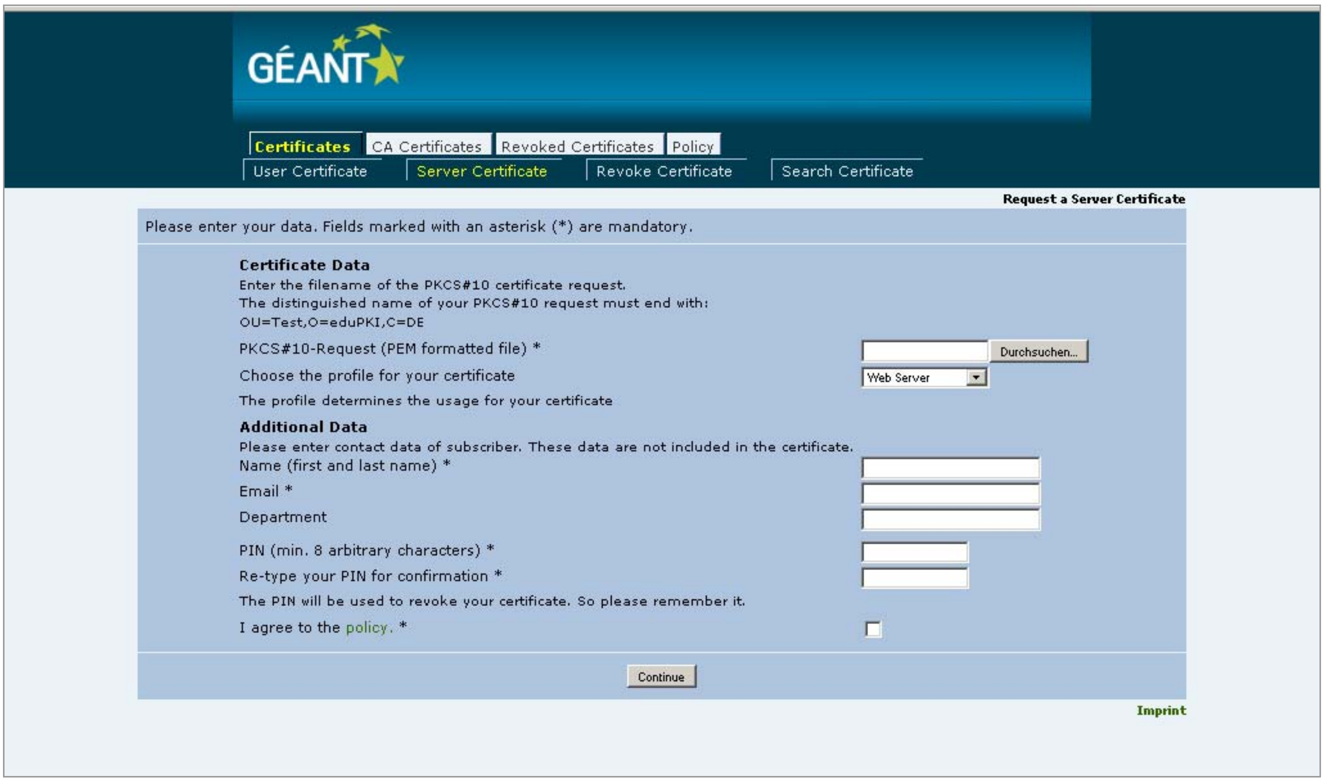
Figure 6: eduPKI flow

Figure 6 above provides a description of the eduPKI service elements and how they interact:

1. A GN3 service presents its security requirements to the PMA.
2. The PMA assesses the service's requirements and either suggests an existing trust profile or prepares a new Trust Profile for the service.
3. The PMA verifies that the NREN CA who wants to issue a Certificate for using the GN3 service complies with the Trust Profile.
4. If the NREN CA complies with the Trust profile, they are added to TACAR, under the Trust Profile.
5. The eduPKI CA supports *all* Trust Profiles defined by the PMA. This CA is added to TACAR and linked to the various certificate profiles.

A.4 Screen-shots of the eduPKI CA Web interface

The figures in this section depict the new eduPKI CA Web interface, developed by SA3-T1.



Request a Server Certificate

Please enter your data. Fields marked with an asterisk (*) are mandatory.

Certificate Data

Enter the filename of the PKCS#10 certificate request.
The distinguished name of your PKCS#10 request must end with:
OU=Test,O=eduPKI,C=DE

PKCS#10-Request (PEM formatted file) *

Choose the profile for your certificate: Web Server

The profile determines the usage for your certificate

Additional Data

Please enter contact data of subscriber. These data are not included in the certificate.

Name (first and last name) *

Email *

Department

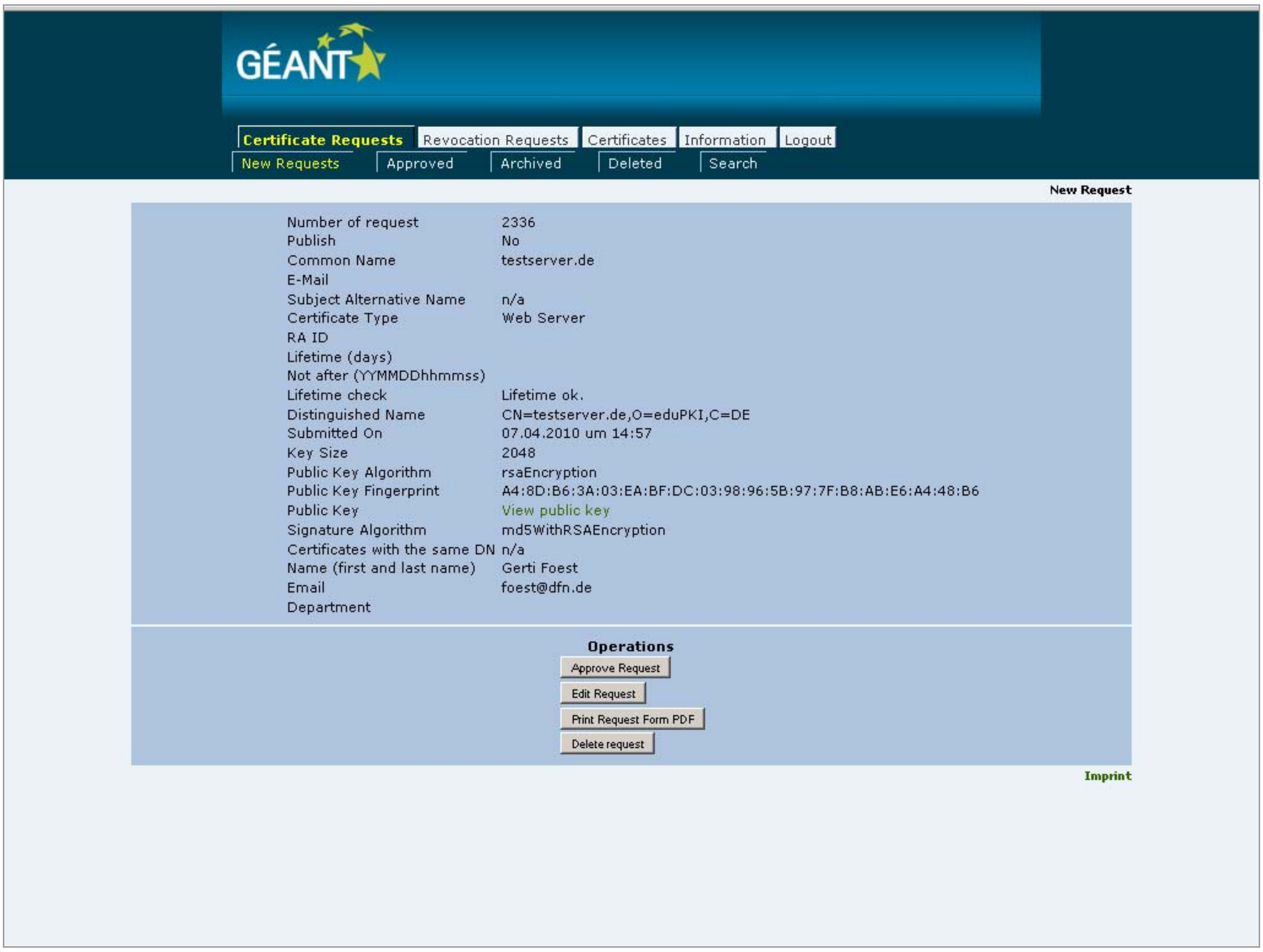
PIN (min. 8 arbitrary characters) *

Re-type your PIN for confirmation *

The PIN will be used to revoke your certificate. So please remember it.

I agree to the policy. * □

Figure 7: eduPKI-CA – Request a Server Certificate



Number of request	2336
Publish	No
Common Name	testserver.de
E-Mail	
Subject Alternative Name	n/a
Certificate Type	Web Server
RA ID	
Lifetime (days)	
Not after (YYMMDDhhmmss)	
Lifetime check	Lifetime ok.
Distinguished Name	CN=testserver.de,O=eduPKI,C=DE
Submitted On	07.04.2010 um 14:57
Key Size	2048
Public Key Algorithm	rsaEncryption
Public Key Fingerprint	A4:8D:B6:3A:03:EA:BF:DC:03:98:96:5B:97:7F:B8:AB:E6:A4:48:B6
Public Key	View public key
Signature Algorithm	md5WithRSAEncryption
Certificates with the same DN	n/a
Name (first and last name)	Gerti Foest
Email	foest@dfn.de
Department	

Figure 8: eduPKI-CA – Details of an active Certificate Request