eduPKI Service Definition

Issuing Date: 25 Feb 2011
Activity: SA3
Task Item: T3 (eduPKI)
Dissemination Level: Public
Authors: L. Florio, J. Howlett

Document Revision History

Version	Date	Description of change	Person
0.1	24-11-2010	First draft issued	L Florio
0.2	11-02-2011	Comments received	J. Howlett
0.3	15-02-2011	New version issued	L. Florio
0.4	18-02-2011	Comments received	O. Kreiter
1	25-02-2011	Final Version	L. Florio

Table of Contents

Executive Summary

The purpose of this document is to provide a high-level description of the eduPKI service's technical and operational model. The intended audience of this document are the GÉANT partners; and in particular the GÉANT services operators that rely on Public Key Infrastructure (PKI) for their operation and service managers responsible for PKI services within the NRENs.

The eduPKI service is not a single service, but is constituted from three different but inter-related elements, the eduPKI Policy Management Authority (eduPKI PMA), the eduPKI Certification Authority (eduPKI CA) and a trust repository (TACAR). These components are described in chapter 3 and 4.

The governance of the eduPKI service, described in chapter 4, is centred on the eduPKI PMA and it is detailed in the document called "edupKI PMA Charter"; this document also explains the relationships among the eduPKI PMA [eduPKI PMA], the eduPKI CA [eduPKI CA] and TACAR [TACAR].

1 Introduction

The goals of the eduPKI service are:

- to support GÉANT services in defining their requirements in respect of the use of digital certificates;
- to co-ordinate the provision of digital certificates to GÉANT services on a Pan-European basis;
- to enable existing Certification Authorities (CAs) to issue certificates for GÉANT services.

2 eduPKI stakeholders

The eduPKI service has the following stakeholders:

- The GÉANT project;
- The project's partners and their CA services (whether operated by the project partners or outsourced);
- The project's services;
- The end-users of the project's services.

2.1 GÉANT Project

GÉANT is a pan-European data network dedicated to the research and education community. The project develops and operates services of common interest to its partners. These services often have requirements for digital certificates, typically for authentication of correspondents and integrity and confidentiality of their data.

The eduPKI service provides the following benefits to the GÉANT project:

- **Coordination on the use of digital certificates throughout the GÉANT project**. The eduPKI service provides a project-level view of its services' requirements of the use of digital certificates, facilitating consistency and best practices across the project.

- **Achieves cost efficiencies and improves the end-user experience**. The eduPKI service provides a framework for federating established CAs, thereby mitigating duplication of infrastructure. End-users are also able to use whichever CA service that they are already familiar with. In this federated model, NRENs remain responsible for the operation of their CAs; the eduPKI service co-ordinates their interactions with the GÉANT services.

- **Avoids the creation of per service-based CAs**. Experience from previous iterations of the GÉANT project demonstrates that service-specific CAs consume resources unnecessarily and hamper the end-user's experience. Little or no manpower is typically allocated for such *ad hoc* CAs, resulting in an unreliable service for end-users.

2.2 Project partners and their CA services

At present there are three principal CAs services[1] operated by the project's partners. One of these services (the TERENA Certificate Service) provides a service to 25 NRENs and their end-users. The eduPKI service enables these CAs to offer digital certificates for the GÉANT services.

The eduPKI service provides the following benefits to the project's partners and their CA services:

- **Provision of support to CAs that wish to participate in the eduPKI service**. This includes, for example, the definition of clear processes and procedures for participation.

- **Creates added value for the CA**. CAs (whether operated by a project partner, or another organisation) are able to offer certificates conforming to the eduPKI service's specifications to their own end-users.

2.3 GÉANT service operators

The eduPKI service provides the following benefits to the GÉANT services:

[1] DFN-PKI, SWITCH-CA and TCS (TERENA Certificate Service)

- **Provision of support to services participating in the eduPKI service**. This includes, for example, the definition of clear processes and procedures for participation;

- **Regular dissemination and meetings with the project's services to understand their requirements**. The eduPKI service seeks to provide GÉANT's services with an efficient and appropriate solution. This reduces their own overheads, as no specific expertise in the area of digital certificates is needed on their side.

2.4 End-users

The end-users, in this context, are the end-users of each of the GÉANT services that the eduPKI service supports. The eduPKI service itself will not have any direct contact with end-users.

The eduPKI service provides the following benefits to end-users:

- **The possibility of using their national CA**. End-users will be able to obtain certificates for GÉANT's services from their national CA (subject to accreditation). This allows them to benefit from this CA's familiar procedures, processes and support;
- **Improved reliability and efficiency**. The central co-ordination of infrastructure, policy and procedures will make services that require digital certificates more reliable and efficient than the case where such co-ordination in absent.

3 eduPKI Service Components

The eduPKI service is not a single service, but is constituted from three different but inter-related elements that are described in the next chapters.

3.1 Policy Management Authority

The Policy Management Authority (PMA) is the cornerstone of the eduPKI service. The role of the PMA is to define, moderate and mediate between the GÉANT services and the participating CAs. On the basis of the services' requirements and PKI best practices and standards, the PMA defines policies called "Trust Profiles"**.** A Trust Profile stipulates the criteria that a GÉANT Service has in respect of its digital certificate requirements.

The CAs operated by the GÉANT partners are, of course, encouraged to issue certificate that conform to these Trust Profiles. However, this requires accreditation by the PMA to ensure that these CAs are issuing certificates in accordance with the relevant Trust Profile(s).

The PMA will, on request, evaluate applicant CAs' procedures to assess their conformance with any of the defined Trust Profiles. The applicant CA, on successfully satisfying these tests, will be accredited under one or more Trust Profiles.

3.2 eduPKI CA

Although the aim is to use existing CAs where possible for the reasons cited previously, there is nonetheless a requirement to operate a CA that issues certificates to all of the project's participants; for example:

- some services may have specific requirements that are not easily supported by existing CAs;
- some end-users may be associated with an NREN that does not provide a CA service.

Consequently the eduPKI service operates a CA that complements the established CA services available to the GÉANT community.

3.3 TACAR

The final element to the eduPKI service is the TERENA Academic CA Repository (TACAR). TACAR maintains a database of root certificates that has become the *de facto* trust repository for eScience. The PMA will announce and publish the accreditation, temporary suspension, or permanent withdrawal of a CA under the relevant eduPKI Trust Profile in TACAR.

3.4 The Service Desk

The eduPKI service operates a website (www.edupki.org) which hosts all the documentation related to the eduPKI PMA work, including any Trust Profile and the eduPKI CA Certificate Policy (CP) and Certification Practice Statement (CPS), and provides links to the eduPKI CA and TACAR websites. The website also provides a contact email address that is used to provide a single point of contact for the participating CAs and GÉANT services.

The TACAR and eduPKI CA websites also offer an email address for requests that are specific to those services.

3.5 Project's Partners and their CA services

The PMA is responsible for supporting the CA operators. It is anticipated that most of the support burden will relate to the processes concerned with participation in the eduPKI service.

The PMA has defined these procedures (also known as accreditation process), how to resolve conflicts and what a CA needs to do to maintain the accredited status.

The '**CA Accreditation Process'** document, available from the eduPKI website, provides more information:

https://www.edupki.org/edupki-pma/pma-governing-documents/

3.6 GÉANT Services Operators

The PMA is also responsible for supporting the GÉANT service operators, and in particular the definition and maintenance of trust profiles associated with the services.

The '**Service Registration Process'** document, available from the eduPKI website, provides more information:

https://www.edupki.org/edupki-pma/pma-governing-documents/

Additional document is also available for GÉANT service operators who wish to make use of the eduPKI CA..

3.7 eduPKI Model

Figure 1 below provides a high-level overview of the eduPKI service model. It is instructive to note the central importance of the PMA; the remaining elements in blue constitute the other elements of the eduPKI service described in the previous sections. TACAR is depicted in lighter blue to indicate that it is not restricted to the eduPKI service or GÉANT project, but it is also used for other purposes.

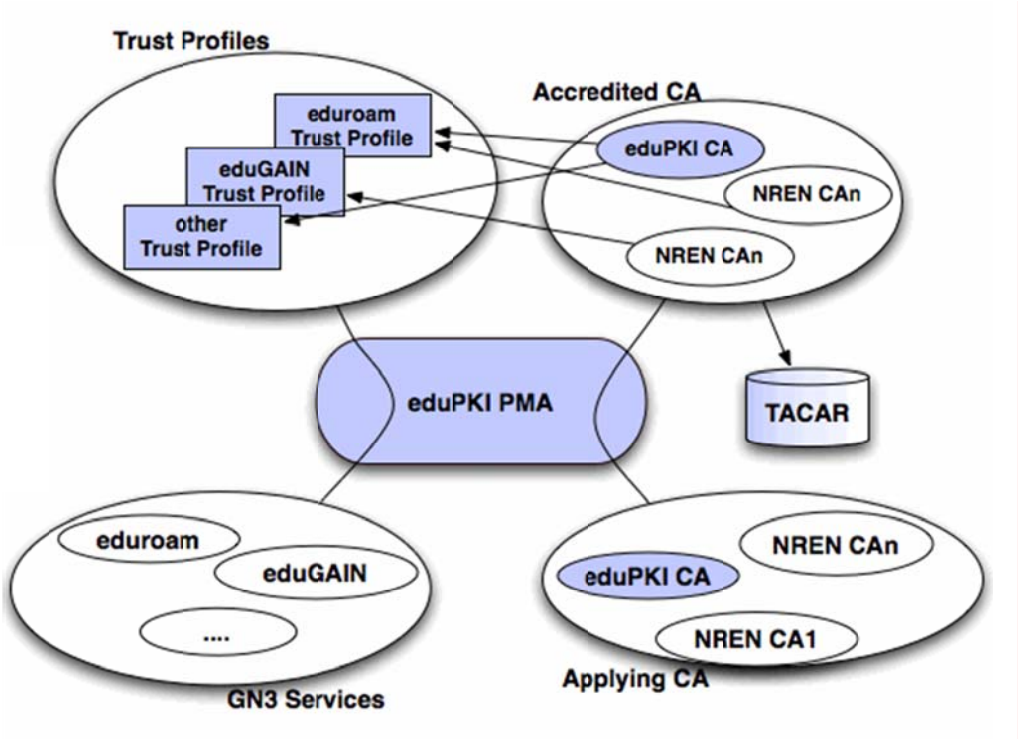

Figure 1: eduPKI Model

4 eduPKI Governance

The eduPKI service has a governance model that is centred on the eduPKI PMA and it is defined in the eduPKI PMA charter. This document explains the relationships among the eduPKI PMA, the eduPKI CA and TACAR.

4.1 The eduPKI PMA

The PMA's governing documents and procedures are defined in the following three documents:

- eduPKI Charter document
- eduPKI PMA GÉANT Services Registration Process document
- eduPKI PMA CA Accreditation Process document

These documents are described in deliverable DS3.1.1 [DS3.1.1], issued in August 2010; the most recent versions of these documents are available on the eduPKI website [eduPKI].

The following sections describe the main aspects of the eduPKI PMA Governance; the reader is advised to refer to the **eduPKI PMA Charter** for a complete description.

4.1.1 PMA membership and structure

A PMA member is an expert that performs one of the functions of the PMA (these functions are defined in the following section). PMA members must belong to a GÉANT partner possess expertise in the area of digital certificates and trust procedures.

New PMA members are appointed by the eduPKI PMA through a voting process; PMA members are expected to share the workload of the eduPKI PMA, although their effort cannot be funded by GÉANT . New PMA members are recruited by invitation or by request from prospective members.

The PMA currently has two members: Milan Sova (CESNET) and Reimer Karlsen-Masur (DFN-CERT Services GmbH); they were appointed by the eduPKI task, which they are also members of.

The GÉANT management is required to appoint one person[2] (plus a back-up for this role) to follow the operations of the PMA.

Figure 2 below depicts the PMA and its relation with the GÉANT project:

[2] Otto Kreiter, GEANT Service Coordinator has been appointed for this role; there is also a backup person for redundancy.

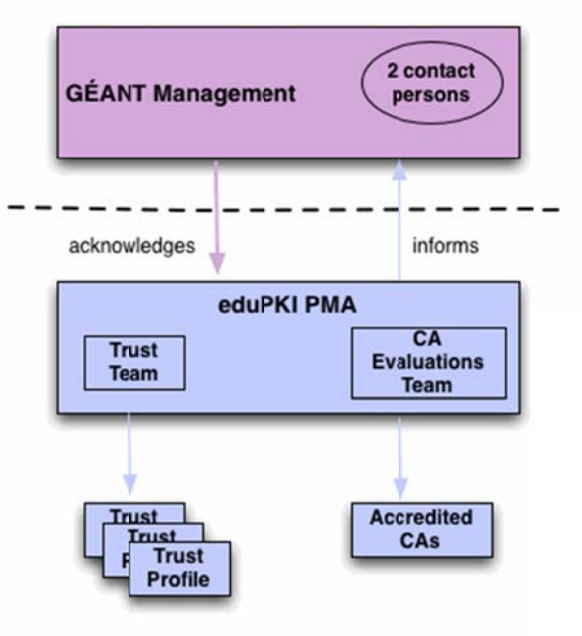

Figure 2: eduPKI PMA Model

4.1.2 PMA tasks

The PMA is responsible for the following main tasks:

- Supporting the GÉANT service operators, and in particular the definition and maintenance of trust profiles associated with the services.
- Supporting the CA operators and in particular enable CAs to become accredited;
- Ensuring that TACAR contains a category for each of the trust profiles.

4.2 CA Policy

The eduPKI CA policy [eduPKI CA] document describes the operation of the CA, the type of certificates issued, the process to validate the certificate requests, and all of the related security procedures.

4.3 TACAR Policy

The TACAR policy [TACAR] defines the procedures for:

- gathering and verifying academic CAs' root certificates;
- publication of these certificates in a central trustworthy repository for download;

TACAR is not a CA, it does not evaluate the policies of the CAs hosted by TACAR; nor does it enforce compliance with any particular technical requirements. These functions rest with the PMA that TACAR works with.

References

[DS3.1.1] http://www.GÉANT .net/Media_Centre/Media_Library/Media%20Library/GN3-10-157-DS3-1-1_Report_on_the_Establishment_Policy_Management_PUBLISHED.pdf

[eduPKI] http://www.edupki.org

[eduPKI CA] https://www.edupki.org/fileadmin/Documents/eduPKI-CA-CP-CPS-1.1.pdf

[eduPKI PMA] https://www.edupki.org/edupki-pma/pma-governing-documents/

[TACAR] http://www.tacar.org