Date: May 2010

Version: Final for Web

SA3 - eduPKI Business Case

Authors: Licia Florio, Reimer Karlsen-Masur, Marcus Pattloch Milan Sova Gerti Foest, Josh Howlett, Ian Thomson, Otto Kreiter

Abstract: The eduPKI Business Case outlines the proposed eduPKI solution to offer a scalable and cost-effective way for the GÉANT project to deal with digital certificates and trust issues in general.

Table of Contents

Executive Summary 2
1 Service Overview 4
2 Strategic Fit 6
3 Options Evaluation 7
4 Affordability 7
5 Achievability 8
6 Annex 1 8
7 Annex 2 9
8 Annex 3 11

Date: May 2010

Version: Final for Web

Executive Summary

The business case for the eduPKI service is set out below; the GN3 Executive committee approved the document in April 2010 to start operations.

During the GN2 project ad-hoc Certification Authorities (CAs) were created, for example eduGAIN CAs. These CAs were not included in the GN2 plans and so no budgeted manpower was allocated to operate them. Consequently the CAs were operated on a best-effort basis, resulting in an unsatisfactory user-experience due to long waiting times when requesting a certificate, and the absence of professional user support. This demonstrated the need for coordination of the GN3 services' security requirements addressed by the proposed eduPKI service.

For these reasons, eduPKI aims to create a GN3 service to support other services by:

1. Defining the GN3 services' security requirements
2. Providing digital certificates[1] to the relevant GN3 services.

These aims of eduPKI will be achieved by creating a framework composed of three different facilities:

i. A dedicated Certification Authority (the Catch-all CA), operated by DFN to match specific requirements and/or to support those NREN users that cannot rely on a national CA service.

ii. An enhanced version of the existing TACAR [2] (TERENA Academic Certificate Authority Repository), to store and distribute the eduPKI participating Certificate Authority's root certificates (including the Catch-All CA root) in a secure manner[2].

iii. Procedures to assess GN3 services' requirements and categorise them into profiles as well as procedures to assess existing national CA operations[3] against the agreed eduPKI certificate profiles and store them into TACAR according to the certificate profiles they match. The Policy Management Authority (PMA) will manage this.

Point (iii) means that eduPKI will build on top of existing NREN CA services, federating them to make all participating CAs, including the catch-All CA, available to the GN3 services. This approach will result in cost reductions (Annex 4) and increased efficiency, as a number of national CAs are already well established and used within the NREN's constituency. The existence of eduPKI will ensure that no manpower is utilised trying to build ad-hoc CAs in various GN3 activities.

End-users will benefit from the eduPKI services because:

i. Due to the proposed federated approach, users of GN3 services will be able to obtain all necessary certificates from either the CA managed by their own NREN (or equivalent service) or via the catch-All CA. It is expected that existing national CAs will implement the profiles defined by the eduPKI service,

ii. End users will have a better user-experience as they will be able to rely on the same type of certificates to access different GN3 services.

1 All certificates follow the well-established X.509 standard. This is the standard that is used by all similar activities worldwide.

2 A root CA certificate univocally identifies a CA and is used to validate certificates purporting to originate from that CA. If a CA is not pre-installed into operating systems and applications, it is necessary to retrieve the root CA.
It is therefore essential to ensure that users relying on certificates issued by a CA can obtain that root CA in a secure manner. TACAR acts as central repository so that users can securely download multiple roots CA at the same time.

3 TERENA Certificates Service (TCS) will be one of the CA assessed.

iii. The certificate delivery time is anticipated to be shorter and service failures due to certificates not being renewed on time will be reduced or eliminated.

iv. For services and researchers, the catch-All CA will offer a possibility to test new features related to the usage of digital certificates and to assess the performances and behaviours of the service.

This business case outlines the proposed eduPKI solution to offer a scalable and cost-effective way to deal with digital certificates and trust issues in general. NRENs are encouraged to join the federated eduPKI service with their eduPKI accredited national CA. This will entail an assessment of the CA procedures and assessment by the PMA. If accredited by the PMA, the root CA will be stored in TACAR and made widely available.

This report shows that the internal cost for NRENs wishing to participate is very low compared to the costs of operating the national CA itself. The expected NRENs internal costs to participate in the eduPKI service only involve the accreditation process to register their CA. This process is expected to require only a few man-days, and will be only needed the first time a CA is registered.

By May 2010, the eduPKI task plans to have:

- A proof of concept of the Catch-All CA for services to experiment with.
- Procedures to accredit NREN operated CAs.
- A trust-repository to store and distribute NREN CAs' root certificates safely.

1 Service Overview

Service goals

The goal of eduPKI is to:

- Create a GN3 service able to support other GN3 services in defining their security requirements concerning the usage of digital certificates.
- To provide digital certificates[4] to the GN3 services.

Examples of GN3 services include: perfSONAR, eduGAIN, eduroam, autoBAHN and any future service with security and trust requirements.

Digital certificates are issued by Certification Authorities (CAs) and are used to guarantee secure and reliable communication between servers, users, or between a user and a server. Examples of this are:

- A user connecting to a Web server securely using a web browser.
- Two users exchanging an email securely.

eduPKI aims to enable GN3 services to obtain digital certificates from CAs operated by NRENs participating in the project that meet the GN3 services' requirements. eduPKI will rely on existing national CAs whenever possible, thus offering a federated service. eduPKI will also offer and operate a dedicated CA to match specific service requirements and/or to support users belonging to an NREN that does not provide a CA service. eduPKI will provide the framework and the procedures to assess GN3 services' trust requirements as well as CA operations, and to ensure that no manpower is consumed trying to build ad-hoc CAs.

The obvious benefits of offering a federated CA service are the cost reductions and increased efficiency due to the fact that a variety of CAs are already well established and used within the NREN environment, and provisions for these CAs has already been made by those NRENs.

The eduPKI will achieve its goal, by providing the following facilities:

1. A **Policy Management Authority** (**PMA**). This will define and maintain a set of criteria that must be met by the participating national CAs. The criteria will be identified on the basis of the GN3 services' requirements. The PMA will accredit candidate national CAs on the basis of an evaluation of their policies and their adherence to the defined criteria. The CAs will then be stored into TACAR according to the certificate profiles they match. The PMA will also support GN3 services in defining and/or reviewing their trust and security requirements. The PMA might also require new features for TACAR.

   The PMA was established in June 2009, with Milan Sova (CESNET) and Reimer Karlsen-Masur (DFN-CERT) as initial members. More information on the PMA can be found at:

   http://wiki.geant.net/pub/SA3/T1EunPKICoordnMain/eduPKI_PMA.pdf

2. A repository built on the existing **TACAR**, which will store and distribute the participating CAs' root certificates in a secure manner. The repository will be operated by TERENA.

   A root CA certificate uniquely identifies a CA and is used to validate certificates purporting to originate from that CA. If a CA is not pre-installed into operating systems and applications, it is necessary to retrieve the root CA. It is therefore essential to ensure that users relying on certificates issued by a CA (not preinstalled) can obtain that root CA in a secure manner. TACAR acts as central repository so that users can securely download multiple root CAs at the same time.

4 All certificates follow the well-established X.509 standard. This is the standard that is used by all similar activities worldwide.

For the last four years TACAR has been extensively tested by the Grid community, which makes extensive usage of digital certificates. Today TACAR is the official trust-repository for the Grid community.

TACAR's model has also been subject to the studies[5] of the IDABC (Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens) as a possible solution to cross-border trust.

3. A "**catch-all" CA** that will provide certificates to users unable[6] to obtain certificates via their NREN-operated CA or to support specific services' requirements. The catch-all CA will be hosted by TACAR and operated by DFN.

Figure 1.1 depicts the relationships among the various eduPKI components, GN3 services and NREN CAs.

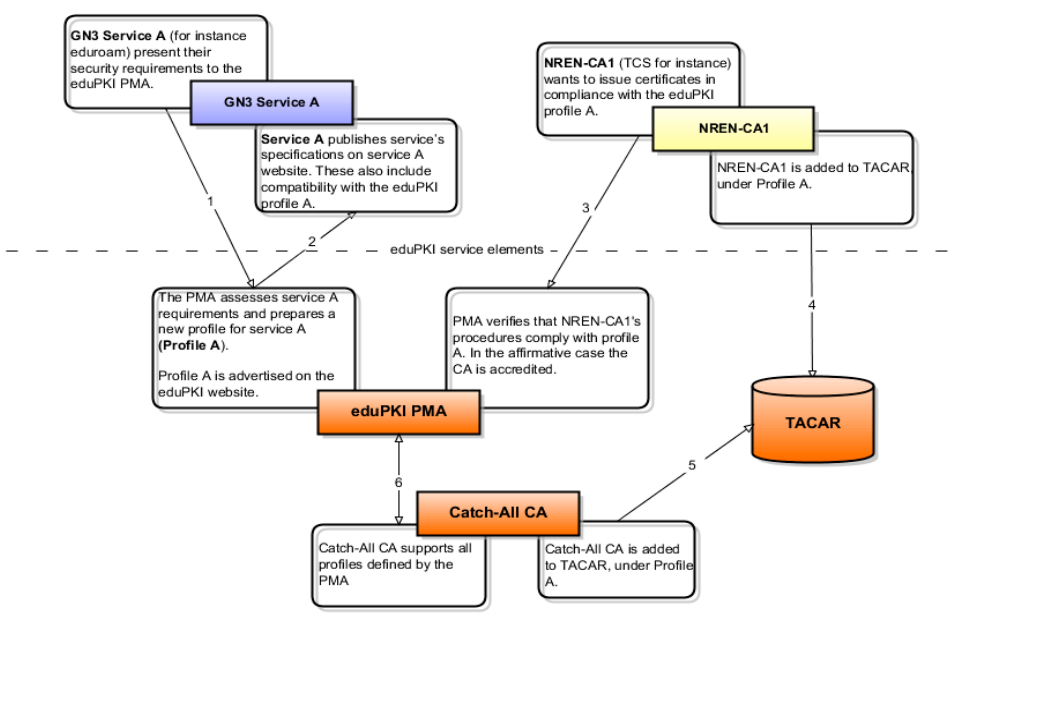

Figure 1.1: eduPKI Service Elements

Service facilities

Breaking down the various eduPKI facilities, the target users' group for each of the facilities is described below:

- The Catch-All CA is expected to target GN3 service administrators. They will be in charge of requesting and installing digital certificates. Requirements concerning the functionalities and the type of certificates that the Catch-All CA should offer are derived from assessing GN3 services. The initial requirements will be refined to include other services requirements, as they become clearer. More information on this is available in the **eduPKI status report** [3].

[5] http://ec.europa.eu/idabc/servlets/Doc?id=32177

[6] The meaning of "unable" is:
- a user belongs to an NREN that does not operate any CA or does not participate in TCS;
- The catch-All CA will not serve a user "belonging" to a NREN operating its own CA, unless a new certificate profile is being tested *(the word test is very important here)* and this test profile is available only via the catch-All CA

- The PMA will target the services' designers and developers to advise them on the best solution that matches their security requirements.
- TACAR is meant to target service administrators, who will benefit from a secure repository to download and install the required CA root certificate(s).
- End-users will benefit from the whole eduPKI for the following reasons:
  a. They will be able to obtain certificates via their national CA.
  b. They will get a better user-experience as users could rely on the same CA procedures and interface and use the same certificate to access different GN3 services;
  c. Certificate delivery time will be reduced, due to the fact that eduPKI will rely on CAs already in existence and operation;
  d. They will not experience service failures because of certificates not being renewed on time.

Use–case identification

To tailor the eduPKI service to GN3 requirements, and to assess the availability of digital certificates at national level, the eduPKI group has conducted a series of interviews with:

- NRENs participating in GN3 and offering digital certificates to their constituency, in order to gather information on policies and procedures of their PKIs.
- The GN3 services[7], in order to gather information on their trust needs and in particular on digital certificates needs.

A summary of the interviews, highlighting the findings and the conclusions, is available in the eduPKI status report. One of the main conclusions drawn from the interviews was that a suitable alternative to replace the operations of the pilot eduGAIN CAs developed during the GN2 project should be provided as soon as possible.

A second round of interviews with the GN3 services is planned for Nov 2010, as most of the services will have clearer trust requirements.

Branding

Note that eduPKI is the task's name, not the marketing name. It is envisaged that TACAR will not be renamed, as it is a well-known service. A name for the Catch-All CA has yet to be decided, and will be addressed separately, during the pilot phase.

2 Strategic Fit

eduPKI will rely, whenever possible, on existing CAs operated by NRENs (or equivalent) participating in the project, thus federating the national CAs.

A centrally coordinated service that federates the national CAs will result in cost reductions and increased efficiency because:

- The same CA might be re-used for different services. This will have the immediate effect of reducing overall operational costs associated with these services. The PMA will provide the coordination framework necessary to ensure that different CAs are able to match different GN3 services' requirements.

[7] eduroam, eduGAIN, perfSONAR services were available for interviews. Other possible GN3 services are still in a design phase and no information was available.

- It will be possible for NRENs and institutions to significantly reduce the complexity of their users' experience in the area of digital certificates, as users could rely on the same certificates to access different services.
- Some special-purpose CAs were created during the GN2 project for specific activities. eduPKI will migrate the services offered by these CAs either to existing CAs or to the catch-all CA.
- The catch-all CA will provide a support service to complement the existing CA services. The catch-all CA would become particularly useful to address the need in a project like GN3 of issuing certificates for users/machines not supported by an NREN's CA.

The success of the services will be measured against Critical Success Factors (CSFs). It is expected that these metrics will be measured on a yearly basis and reported in the yearly GN3 report. The exact methodology will be developed in the final service definition following the trial phase.

3 Options Evaluation

The Task evaluated the following four options that could have provided a solution to the GN3 services' digital certificate requirements:

1. Do nothing i.e not to make this a dedicated topic in the GN3 project.
2. Acquiring the necessary certificates from a commercial CA.
3. Acquiring the necessary certificates via the TERENA Certificate Service (TCS) [4].
4. Creating a GN3 "trust factory" to manage the project's requirements for digital certificates.

The options and an overview of their evaluations are presented in Annex 2.

After careful analysis and investigation the decision was made to pursue the option to create a GN3 service to manage the project's requirements for digital certificates (option 4).

4 Affordability

eduPKI is a fairly small task with a total of 6,15 FTEs over 4 years. DFN, TERENA and CESNET are the only NRENs participating in eduPKI.

It is estimated that the total cost will not increase by increasing the number of GN3 services requesting certificates, or the absolute number of certificates requested.

It is also expected that the costs for each NREN CA participating in the federated eduPKI to be quite insignificant compared to the costs of operating the CA itself. The only cost envisaged for NRENs is to undergo the accreditation process to register their CA within the eduPKI. This process is expected to require only a few man-days and is generally only needed the first time a CA is registered. The accreditation process will be detailed in a dedicated document due in April 2010.

5 Achievability

eduPKI can be considered a meta-service, designed to support other services. One of the risks associated with the eduPKI task lies in the fact that the eduPKI builds on the GN3 services' requirements concerning trust and digital certificates. If GN3 services do not provide proper trust requirements to the eduPKI PMA, or if delays occur on the services' side in establishing these requirements, this might have implications on the quality of the work of eduPKI.

Another risk associated with eduPKI is the possibility that the demand for certificates from GN3 services might be lower than expected, due to factors like new services' specifications or low take up of these services in the GN3 community.

This risk will be managed by

- Regularly approaching GN3 services (through interviews) to assess the evolution of their trust requirements. The first round of interviews was concluded in November 2009; a new series of interviews is expected in November 2010.
- Awareness on the scope of eduPKI facilities will be raised via presentations, news items, and during the GN3 project meetings.

One of the highest costs of the eduPKI service is related to the operation of the catch-all CA. The risks associated with the catch-all CA are, however, limited because:

- This CA will only be created following an assessment of the current GN3 services' needs, and of those of services already planned.
- Initially the catch-all CA will be implemented as a proof of concept (expected in April 2010) to demonstrate the feasibility and the functionalities over a Pilot period of between six to 12 months. Feedback will be collected through the Pilot to assess its success. Transition to service will only be planned on the basis of the services' requirements.

TACAR specifications to enhance the current TACAR system were developed in November 2009 [5], so the new version of TACAR will be available in April 2010.

By May 2010, the eduPKI task plans to have a proof of concept for the Catch-All CA for services to experiment with, procedures to accredit NRENs operated CAs and a trust-repository to safely store and distribute NRENs CAs' root certificates.

6 Annex 1

[1] A more detailed service description is available at:

http://wiki.geant.net/bin/view/SA3/T1EunPKICoordnMain

[2] TACAR, the TERENA (http://www.tacar.org) Academic Certificate Authority repository, has been developed by TERENA as cost-effective way to address the problem of collecting and distributing root CA in a secure fashion. A high-level description of TACAR is available at:

http://wiki.geant.net/pub/SA3/T1EunPKICoordnMain/tacar_description_v0_1.pdf

[3] eduPKI Status Report can be found at:

http://wiki.geant.net/pub/SA3/T1EunPKICoordnMain/StatusReporteduPKI_v1_0.2-final.pdf

[4] In 2006 TERENA, on behalf of a number of participating NRENs, contracted a commercial CA to issue server certificates [2] to the Research and Education community served by these NRENs. The service was known as TERENA Server Certificate (SCS).

As result of the success of this service, a Call for Proposals was issued in 2008 to renew the initial contract, and a successful bidder was selected. Participating NRENs can continue to obtain server certificates, as well as client and code-signing certificates offered by a commercial CA. This service is known as TERENA Certificate Service, or TCS.

The key benefit of TCS is that the chosen CA's root certificate is pre-installed in most of the commonly used operating systems.

The full list of NRENs participating in TCS is available at:

http://www.terena.org/activities/tcs

[5] New TACAR specification collected in October-November 2009:

http://wiki.geant.net/bin/view/SA3/NewSpecificationsForTACAR

7 Annex 2

The options and an overview of their evaluations are presented here:

1. Do nothing i.e. not make this a dedicated topic in the GN3 project.
2. Acquiring the necessary certificates from a commercial CA.
3. Acquire the necessary certificates via the TERENA Certificate Service (TCS) [4].
4. Create a GN3 "trust factory" to manage the project's requirements for digital certificates.

1. **Do nothing i.e. not to make this a dedicated topic in the GN3 project.**

   This approach has the advantage of saving the expenditure allocated for the eduPKI task, but it most likely will result in the creation of more ad-hoc CAs. This will consume GN3 resources, and will increase complexity for users, institutions and NRENs alike. Furthermore, services will work in isolation, running the risk of duplicating effort. The GN2 project clearly demonstrated this.

   During the GN2 project some ad-hoc CAs were created, an example of this being the eduGAIN-SCA. Because no provision was made to support this CA, manpower allocated for eduGAIN had to be consumed. Furthermore the CA has only operated as a pilot and currently there are no resources allocated to support it. The implication of this is that other services depending on the eduGAIN-SCA, (such as GEANT IdP and perfSONAR) were affected by the lack of procedures to renew their certificates during the summer of 2009.

2. **Acquiring the necessary certificates from a commercial CA**.

   Using a commercial CA would offer the benefit of using certificates that are pre-installed into applications and operating systems. Because each and every certificate would have to be bought independently, this option would become costly if a large number of certificates were needed.

Note:

- The cost for a one-year server certificate might vary depending on the CA.
- In addition, some services might have special needs (e.g. including URNs in their certificates), which might not be fulfilled by commercial CAs. It is also not clear whether using commercial certificates would lead to much stricter rules when issuing certificates.
- Lastly, the increased costs (depending on the number of certificates) might have implications on the ability to perform tests with technologies based on digital certificates, which would not be desirable (especially in research activities). This would have obvious implications on the overall quality of work.

3. **Acquire the necessary certificates via the TERENA Certificate Service (TCS) [4].**

Although this option might appear quite attractive, some considerations should be taken into account:

- To date, 20 NRENs participate in TCS. All of the 20 NRENs are able to acquire server certificates via TCS. Only a fraction of them has opted in to acquire client certificates as well. Although TCS covers a significant number of NRENs, not all the NRENs participating in GN3 have joined TCS.
- Asking NRENs to join TCS would be neither a desirable nor a realistic option. Joining TCS requires a yearly fee to be paid, as well as dedicated manpower to operate the service at national level. In some cases, NRENs have rolled out a national CA service based on different providers and would be unlikely to join another service.
- For smaller NRENs this option would not be sustainable, as it would involve extra costs.
- If an NREN expects to request less than 10 certificates per year, then TCS would not be a convenient option.
- As for the option 2, some services might require specific fields in their certificates, which would either not be available via TCS or would otherwise be available at a much higher price.

4. **Create a GN3 "trust factory" to manage the project's requirements for digital certificates.**

- This option will reduce the complexity and business overheads associated with operating multiple special purpose CAs. However, because of the way eduPKI is conceived, NRENs participating in TCS or other NRENs like DFN and SWITCH (which have deployed national solutions) would still be able to use their certificates. The catch-all CA would complement and complete the picture.
- The eduPKI task will also help services by using the expertise of the PMA members look at the trust aspects when designing services, without each of the services having to develop their own expertise in the area.
- In the context of this task, TACAR should be seen as a support tool, to distribute root certificates [3]. The benefits of using TACAR relies on the fact that TACAR has been used for years to store and distribute Grid root certificates, and therefore the PKI experts in the community are already familiar with such a tool. Furthermore TACAR would become a cross-activity (Grids, GEANT/NRENs) repository, which would be useful.

In summary, the preferred option is option 4, to create a GN3 "trust factory" to manage the project's requirements for digital certificates**,** as it:

- Fits into the model of having a dedicated service that provides the trust model for other federated services.
- Allows for flexibility in defining certificates.
- Allows for an unlimited number of certificates (both server and clients).

- Does not impose obligations on the NRENs concerning the issuing CA, allowing those NRENs that have already a national PKI to use that.
- Provides a facility to also support smaller NRENs.

8 Annex 3

The table below shows the total manpower for the eduPKI task as well as the names of the participants.

NREN	FTE over 4 years	Name of participants
TERENA	2,15	Licia Florio, Christian Gijtenbeek
DFN	3	Marcus Pattloch, Gerti Foest, Reimer Karlsen-Masur
CESNET	1	Milan Sova
TOTAL	**6,15**	

Table 8.1: eduPKI Total manpower