MS3.1.2 Status Report

Last updated: 17-12-2009
Activity: SA3-T1
Dissemination Level: Internal
Document Code: GN3-09-270
Authors: Licia Florio

Document Revision History

Version	Date	Description of change	Person
0_1	15-10-2009	First draft issued	L. Florio
1_0	07-12-2009	Included findings from interviews to NRENs and GN3 services	G. Foest, R. Karlsen-Masur, L. Florio
1_0.1	10-12-2009	Final version	
1_0.2	17-12-2009	Template updated, final editing.	I. Thomson

Table of Contents

1	Aim of the document	3
2	eduPKI Goal	4
3	eduPKI Service Components	5
	3.1 eduPKI Policy Management Authority (PMA)	6
	3.2 TACAR	6
	3.3 Catch-all CA	7
4	Results from the interviews with NRENs and GN3 services	8
	4.1 Summary from the Interviews with NRENs and TERENA offering PKI services	10
	4.2 Services demands	10
5	Conclusions and Next Steps	13
6	References	14

1 Aim of the document

This document provides an overview on the work carried out within the eduPKI task in the first eight months of the GN3 project. The document describes the service that eduPKI is preparing to offer to other GN3 services/activities.

Part of the work carried out by the eduPKI group focused on collecting trust requirements from the various GN3 services or potential services. This document only addresses the requirements concerning the needs for digital certificates. During the discussion with the GN3 services, requirements were also collected concerning the usage of a trusted repository to securely store and exchange trust tokens. These requirements will be collected in a future document, which will define the speciation to enhance the current TACAR.

Links to related eduPKI documents are also provide within this document.

2 eduPKI Goal

The goal of the eduPKI service is to create a “Trust factory” able to support GN3 services in defining their trust requirements and to provide digital certificates[1] to GN3 services whenever needed.

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

The GN3 services are expected to be the main beneficiary of the eduPKI service, as they will be able to obtain certificates through eduPKI's service rather than creating and running their own ad hoc and service-specific Certificate Authority.

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

- NRENs participating in GN3 and offering digital certificates to their constituency to gather information on policies and procedures of their Public Key Infrastructures (PKIs).
- With the GN3 services needs to gather information on their needs for digital certificates and more in general concerning services security needs.

A summary of the interviews highlighting the findings and the conclusions is reported in section 4 “Results from the interviews with NRENs and GN3 services”.

It is worth noting that to facilitate adoption of eduPKI by GN3 services, eduPKI intends to rely (as much as possible) on national PKIs already deployed by NRENs in Europe. eduPKI will create the procedures and the entity (the Policy Management Authority, PMA; see 3 “eduPKI Service Components”) to accredit existing CAs to issue certificates to support GN3 services and to make GN3 services aware of the CAs they can rely on.

However, those NRENs that do not have a national PKI service will be supported through a special purpose”Catch-All” PKI. The interviews with both GN3 services and NRENs operating a PKI are therefore essential to shape and scope the eduPKI service.

A more detailed service description and a business case have also been prepared. These documents are being discussed by the GN3 management and as soon as they are approved they will be available at:

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

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

3 eduPKI Service Components

To achieve its goal, eduPKI will provide the following facilities:

1. A Policy Management Authority (PMA) that will define and maintain the set of criteria that must be met by the participating CAs. It will accredit candidate CAs on the basis of an evaluation of their policies and their adherence to these criteria.
2. A repository, built on the existing TACAR that will store and distribute the participating CA certificates in a secure manner.
3. A Catch-All CA that will provide certificates to users unable to rely on an NREN CA.

The picture below depicts the relations among the various components. The elements in orange are eduPKI's responsibility.

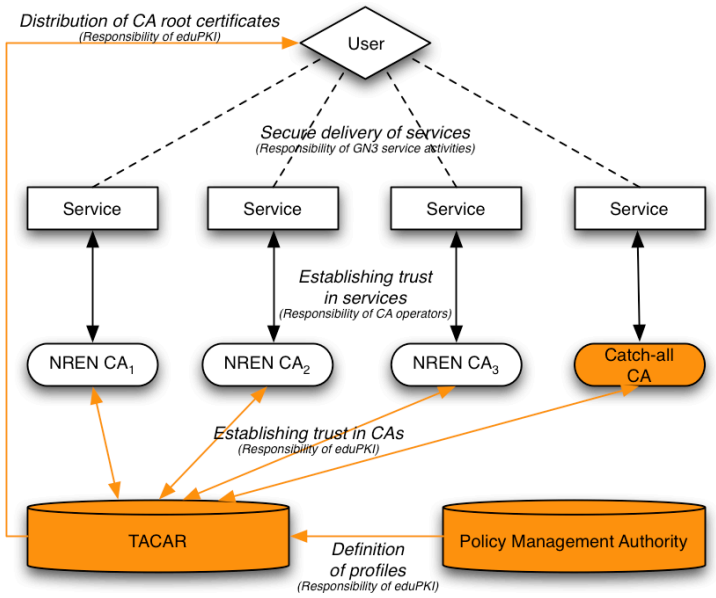

Figure 3.1: The eduPKI service elements

3.1 eduPKI Policy Management Authority (PMA)

The aim of the eduPKI Policy Management Authority (PMA) is to define and maintain the set of criteria that must be met by participating CAs. The PMA will accredit candidate CAs on the basis of an evaluation of their policies and their adherence to these criteria.

The PMA has different tasks, such as:

- Assessing GN3 services' requirements;
- Assessing existing NREN-operated CAs' policies against GN3 services' requirements;
- Defining some **Profiles**, which will indicate the minimum requirements that a CA must fulfil 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.
- 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 NRENs CA should be stored and maintained into the repository (TACAR).

The PMA was established in M3 (June 2009) of the project. It was agreed that Milan Sova (CESNET) and Reimer Karlsen-Masur (DFN-CERT) would be the initial members of the PMA. It is not planned for accredited CAs to automatically become a member of the PMA, though experts from CAs/NRENs can become a member if they are willing to take over some of the workload of the PMA. More information about the PMA is online at:

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

A **PMA Charter** is under preparation and will describe the procedures for the tasks above. It will also define the administrative structure and the basic operation of the PMA. The first draft of PMA charter is expected in October 2009.

3.2 TACAR

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

TACAR, the TERENA Academic CA repository, is already used to store this type of root certificates and to make them available for download in a secure manner.

TACAR will be enhanced to provide a better user interface and to operate according to the recommendations provided by the PMA. The typical end-users of TACAR are application and web administrators.

A new version of TACAR is scheduled for by April 2010 (M12). The new TACAR specifications are determined by assessing the requirements of GN3 services.

Dedicated videoconferences are being held by the eduPKI group to discuss the use-cases that TACAR ought to support. Requirements have been collected from eduGAIN, eduroam and perfSONAR as well as those coming from the eScience community that is already using TACAR.

A document defining the specifications for the new TACAR is under preparation and will be available at the beginning of 2010.

More information on the current TACAR functionalities is available on line at:

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

3.3 Catch-all CA

The Catch-all CA is intended to issue certificates to those end-users and GN3 services that cannot, for whatever reason, rely on a national CA. The level of demand for a Catch-all CA is being clarified by the interviews with the GN3 services; the interviews concerning the services' requirements, and as a result the capabilities of NRENs' CAs are becoming better understood.

The eudPKI group has also investigated the status and the usage of CAs created during the GN2 project. An example of which is the eduGAIN CA, operated by RedIRIS[2]. The eduPKI group has liaised with RedIRIS to gather information on the type of certificates issued by this CA, on the GN3 services relying on this CA and based on this has started a migration plan to move the operations of the eduGAIN CA to the eduPKI group. The Catch-All CA could therefore offer, among others, eduGAIN CA capabilities.

A Catch-All CA pilot is expected to start in April 2010.

[2] RedIRIS is operating the eduGAIN as best effort; no manpower has been allocated to RedIRIS for this purpose.

4 Results from the interviews with NRENs and GN3 services

To be able to tailor the eduPKI service according to GN3 services' requirements it was necessary to get a picture of the current situation. For this purpose two questionnaires were developed to collect the following information:

1. **Availability of PKI Services, and more precisely:**
   - Which NRENs participating in the GN3 project (or equivalent institutions) are currently operating PKI services to provide the academic community with certificates or plan to do so in the near future?
   - What are the organisational frameworks in which the PKI services operate (constituency, structure of PKI, policy, type of identification procedures, audits etc.)?
   - How are the PKI services operated (online CA, kind and number of certificates issued, validity period of certificates, support of crypto-token, pre-installed in standard browsers etc.)?

2. **GÉANT Services trust requirements and more precisely:**
   - Which services use certificates for their authentication procedures?
   - How do the services currently obtain their certificates (who issues the certificates, what are the procedures to obtain a certificate etc.)?
   - What are the demands of the services (level of identification, certificate profiles, validity period etc.)?
   - Are the demands met by the currently used PKI service?

The questionnaires were sent to people known to be involved in either PKI activities in their NREN or in GÉANT services prior to face-to-face interviews with the respective contact persons and members of the eduPKI team. These interviews were mainly conducted via videoconferences, but also in person at conferences and workshops. The interviews provided the opportunity to discuss the questions and the related answers and get a better understanding of the issues on both sides.

Interviews have been conducted with:

- Seven NRENs, two institutions and TERENA offering PKI services (see Table 4.1).
- Three GÉANT services using certificates (see Table 4.1).

Table 1 below gives an overview of the results of the interviews. The next chapters provide an analysis of the findings.

	Offers / Requirements (including those optional)	PKI Services															Demands of Services					
		DFN			CESNET	rediRIS	SIGMANET	GARR	TERENA		GRNET	SWITCH			SRCE (CARNET)	eduGAIN SCA(1)	eduGAIN		eduroam		perfSONAR	
		Global	Grid	SLCS					SCS	TCS		SSL	Grid	SLCS			curr.	plan	curr.	plan	curr.	plan
1.	X.509 Certificates	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	?	√		√	
2.	Kind of certificates																					
	Server (S)	√	√	X	√	√	√	√	√	√	√	√	√	X	√	√	√		√		X	
	User (U)	√	√	√	√	√	√	√	X	√	√	X	√	√	√	X	X		√		√	
3.	Usage of certificates																					
	Server authentication	√	√	X	√	√	√	√	√	√	√	√	√	X	√	√	√		√		X	
	Client/user authentication	√	√	√	√	√	√	√	√	√	√	X	√	√	√	X	√		√		√	
	Encryption	√	X	X	X	X	X	X	X	X	√	√	√	√	X	X	X		√		X	
4.	Level of identification																					
	Face to face identification	√	√	√	√	√	√	√	√	√	√	X	√	X	√	?	√		√		?	
	Verification by postal addr.	X	X	X	X	X	X	X	X	X	X	X	X	X	X	?	X		X		?	
	Verification by email addr.	X	X	X	X	X	X	X	?	?	X	√	√	X	X	?	√		√		?	
5.	Certificate profiles / specific parameters																					
	URN	√	X	X	X	X	X	X	X	X	X	X	X	X	X	√	√		√	–	X	
	OID (additional to policy OID)	√	X	X	√	√	√	√	√	√	√	√	√	√	√	√			–	√	X	
6.	Max. Validity period (end entity Certs)																					
	< 1 mill. seconds	–	–	X	X	X	X	X	X	X	X	X	X	X	X	X	X	?	X		√	
	1 mill. seconds	–	–	√	X	X	X	X	X	X	X	X	X	√	X	X	X	?	X		X	
	12 months	–	–	X	–	√	√	√	√	√	–	√	√	X	–	√	√	?	√		X	
	13 months	–	√	X	√	X	X	X	√	√	–	–	X	X	√	X	√	?	√		X	
	24 months	–	X	X	X	X	X	X	√	√	√	√	X	X	X	X	√	?	√		X	
	36 months	√ (U)	X	X	X	X	X	X	√	√	X	√	X	X	X	X	√	?	√		X	
	60 months	√ (S)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	√	?	√		X	
7.	Globaly coordinated namespaces	X	√	√	√	√	√	√	X	?	X	X	√	√	√	X					X	
8.	HSM	√	√	√	√	X	X	X	√	√	√	√	√	√	X	X						
9.	Online CA	√	√	√	√	X	X	X	√	√	√	√	√	√	X	X	√		√		√	
10.	Reaction time																					
	best effort	–	–	X	–	√	√	√	–	–	–	–	–	X	√	√						
	automatic after approval	√	√	X	√	X	X	X	√	√	√	√	√	X	X	X	√	?	√	√		
	fully automatic	X	X	√	X	X	X	X	X	X	X	X	X	√	X	X					√	
11.	SmartCards or crypto token	√	X	X	√	X	X	X	X	X	√	X	X	X	X	X	X		X		X	
12.	Key-backup/recovery	√	X	X	X	X	X	X	X	X	?	X	X	X	X	X	X		√		X	
13.	PKI Policy available/needed	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√		√		X	

Legend:

√		Service: Demand PKI: Offered
√		PKI: can be offered on demand
X		Service: no demand PKI: not offered
?		PKI: not clear if offered
?		Service: under discussion; not yet decided
–		not applicable

[1] EduGAIN SCA is an ad hoc-CA created during GN2 project. It is listed here for completeness

Table 4.1: Interviews' summary

4.1 Summary from the Interviews with NRENs and TERENA offering PKI services

The response from the NRENs operating PKIs was very positive and gave a good picture of the state of the art.

In summary the following could be concluded:

- All PKI services offered by NRENs have a formal policy.
- Many PKI services are compliant to IGTF minimum requirements.
- CAs usually perform identity vetting by personal identification (face-to-face);
- Most of the PKI services issue server as well as user certificates.
- Most of the PKI services run online CAs (and use HSMs to secure their private key material).
- Key escrow/backup support is offered rarely.
- Two PKI service operated by an NREN and TERENA have their root certificates included in standard browsers.

Most of the PKI services have been established because of Grid use-cases and are therefore compliant with the requirements defined by the IGTF. Often these IGTF-compliant PKI services issue certificates for usage other than Grid. Some NRENs operate PKI services offering several CAs for different purposes that differ from the IGTF standard, especially in respect to the validity period of certificates.

All PKI services (except eduGAIN CA) are established on a long-term basis and are operated by dedicated staff. eduGAIN CA was established specifically for the purpose of providing certificates for eduGAIN (also used by euduroam) and is not meant to operate on a long term basis. In fact RedIRIS (who operate the CA at the moment) does not have any assigned manpower within GN3 for this task. The eduGAIN CA still operates as a pilot.

4.2 Services demands

The response from the GÉANT services was not as satisfactory as hoped. The eduPKI group tried to interview all GÉANT services, but answers were only provided by eduroam, eduGAIN and perfSONAR. The level of information concerning their PKI requirements provided by each of the services varied significantly.

In the **eduroam** case, the interview resulted in clear requirements, which define the scenario that the eduroam group is aiming at in the near future. eduroam currently uses URIs in their certificates to identify RADIUS nodes. The eduroam development team plan to replace the URIs with PolicyOIDs (and probably SRV records), which would make the use of the URN registry unnecessary.

During the interview the **eduGAIN** group clearly expressed a need for certificates that would be used by the participating federations to sign the metadata that they publish to eduGAIN. These certificates will be self-signed, and so it would be necessary to establish trust in these out-of-band. There is therefore a requirement for a PMA profile that defines the policy controlling these certificates, even if these are not issued by a recognised certificate authority. It will therefore be necessary to establish appropriate processes to ensure

reliable and trustworthy exchange of information between eduPKI and eduGAIN. The certificates within the eduGAIN metadata that are associated with entities are out-of-scope of eduPKI.

The trust requirements become less clear in the case of **PerfSONAR**. During the GN2 project, three dedicated eduGAIN profiles [1] were developed to support the non-Web authentication scenario, which applies to both PerfSONAR and AutoBAHN. Specifically, the profiles address the case in which a user (or a host) authenticates to their IdP not using a web-browser.

The profiles make use of SASL CA, which retrieves the appropriate attributes from the user's IdP and creates a certificate for the user/host. An online eduGAIN CA (called eduGAIN OCA) was created to issue certificates for the SASL CA (Figure 4.1). It was not clear how many SASL CAs are operational to date; in fact it may be very possible that the only SASL CA in operation would be the one operated by DANTE as part of the GIdP.

There seems to be a plan to phase out the SASL CA out, but during the interview no sufficient information on this point could be provided. From the eduPKI's perspective, there is a need to fully understand whether there is a requirement for a SASL CA, in order to cater for that when migrating the eduGAIN CA.

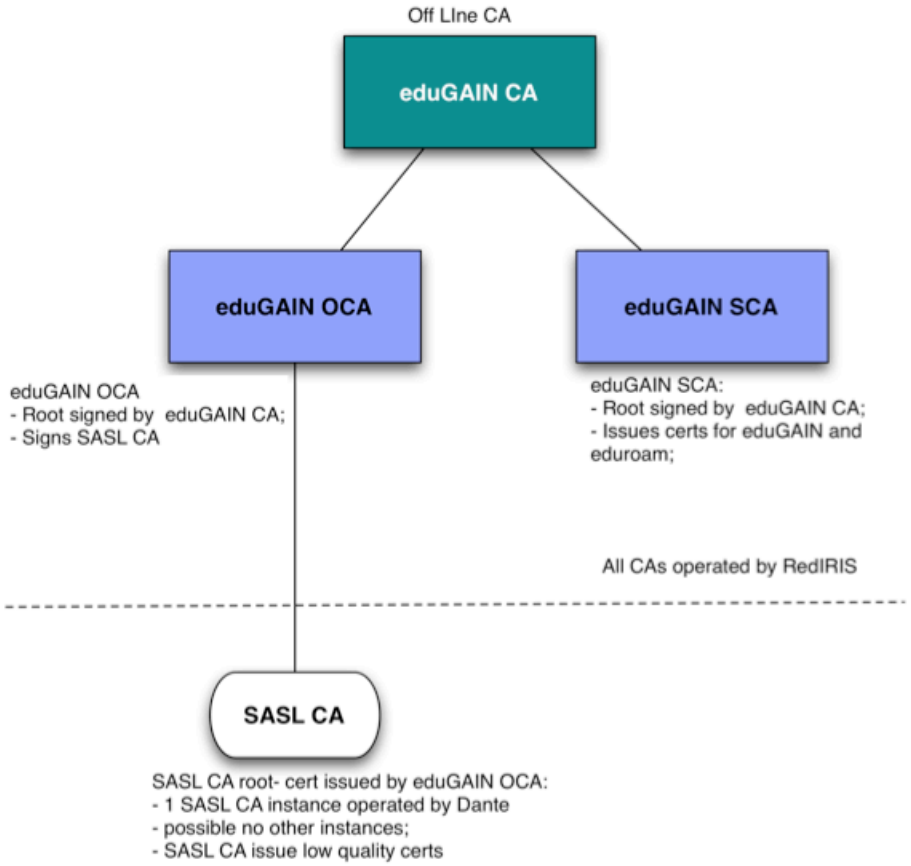

Figure 4.1: eduGAIN CA hierarchy

In summary, during the interviews it was possible to identify the following common requirements:

- GÉANT services that obtain their certificates from existing PKI services reported a satisfactory experience.
- Except for very special use cases, the users are looking for long certificate validity periods.
- Key escrow/backup support is not a demand.
- There is a demand for short reaction time when requesting certificates.
- Easier procedures to obtain certificates and shorter reaction time to certificate requests are an issue, which was mostly highlighted by the services relying on the eduGAIN CA.
- The method of identity vetting is not an issue; email address verification is accepted as well as personal identification (face-to-face).
- Server/client as well as user/client certificates are required by some of the services but not by all of them.

5 Conclusions and Next Steps

A number of PKI services exist in the European NREN community that are able to issue certificates to their users for different purposes. However, the demands from the GÉANT services are not completely clear at the time of this report, and do not cover all the services planned under GN3. Therefore it was not possible to come to a final conclusion about how the GÉANT services could be served best by eduPKI.

There is a clear demand to migrate the existing eduGAIN CA to a persistently operated CA with dedicated manpower. This includes not only a transition of the current infrastructure to a different operating team, but also redefining the CA policies, operations and user interfaces. Because of the lack of requirements from other GEANT services (such as authoBAHN and to a certain extent perfSONAR), the eduPKI group will design a catch-all CA based on the requirements coming from eduroam and eduGAIN. A further discussion with these two services and all the others not available for the interviews is needed to clarify their requirements.

A Catch-All CA pilot is expected to start in April 2010.

To minimise the risks, the catch-All CA will initially operate as a proof of concept and will be built upon eduroam and eduGAIN requirements.

Ongoing dialogue with the GÉANT services and a final conclusion in respect to the demanded eduPKI service will be the subject of the next work period of the task.

6 References

[1] **eduGAIN nonWeb profiles:**
AC -> Automated client (an autonomous process)

UbC -> User behind a Client (for non-Web clients)

WE -> Web-Enhanced (for web applications acting on behalf of a user)

They are defined in “Best Practice Guide - AAI Cookbook - Third Edition”, http://www.geant2.net/upload/pdf/GN2-08-130-DJ5-2-3-3_eduGAIN_AAI_CookBook-1.pdf