eduPKI
Policy Management Authority
Charter

Version 1.0

23.08.2010

Abstract

This is the Charter of the eduPKI Policy Management Authority (eduPKI PMA). The eduPKI PMA is a group of technical experts within GÉANT that is vetting certification authorities as part of Public Key Infrastructures which issue X.509 digital certificates for use within the GÉANT community according to rules and practices set as minimum criteria which are defined by the eduPKI PMA. This document describes how the eduPKI PMA is set-up and operated, its scope, objectives, activities and voting processes.

Change History

Version	*Author*	*Date*	*Changes*
1.0	RKM	23.08.2010	Init

Table of Contents

1 Scope and Objectives of the eduPKI PMA

This Charter document describes how the eduPKI Policy Management Authority is set-up and operated, its scope, objectives and responsibilities, membership and voting processes.

The eduPKI Policy Management Authority (hereafter called eduPKI PMA) is a group of technical experts within GÉANT that gathers trust fabric requirements from GÉANT Services that wish to deploy or use asserted identities based on X.509 digital certificates issued by a Public Key Infrastructure (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 *eduPKI Trust Profiles*, represent the different requirements, trust characteristics and identity assertions that GÉANT Services have in regards to their authentication needs. The eduPKI PMA defines one or more common eduPKI Trust Profiles that are acceptable to GÉANT Services.

Furthermore the eduPKI PMA evaluates applying PKIs with their associated Certification Authorities (CAs) in regards to their conformance with any of the defined eduPKI Trust Profiles. Based on the positive outcome of such an evaluation an applying CA is accredited under one or more eduPKI Trust Profiles and the details of the CA are published by the eduPKI Trust Anchor Repository.

The eduPKI PMA acknowledges emerging new trust patterns and authentication technologies within the GÉANT community and in due course may amend the scope of the eduPKI PMA to include and cater for these if there is a sustainable demand and user base.

Thus the eduPKI PMA defines, moderates and mediates the trust domains between the GÉANT Services, its users and the identity assurers namely the CAs.

2 Identification of this document

Name: eduPKI PMA Charter

Version: 1.0

Date: 23.08.2010

3 Contact Information

The eduPKI PMA office can be contacted via various means:

Web-site: www.edupki.org

Email: pma@edupki.org

Mail: eduPKI PMA
c/o DFN-Verein
Alexanderplatz 1
10178 Berlin
GERMANY

4 Structure of the eduPKI PMA

The eduPKI PMA consists of the eduPKI PMA Board whose members supported by Teams perform various activities. The GÉANT management endorses and installs the eduPKI PMA. An overview of the eduPKI PMA structure is given in illustration 1.

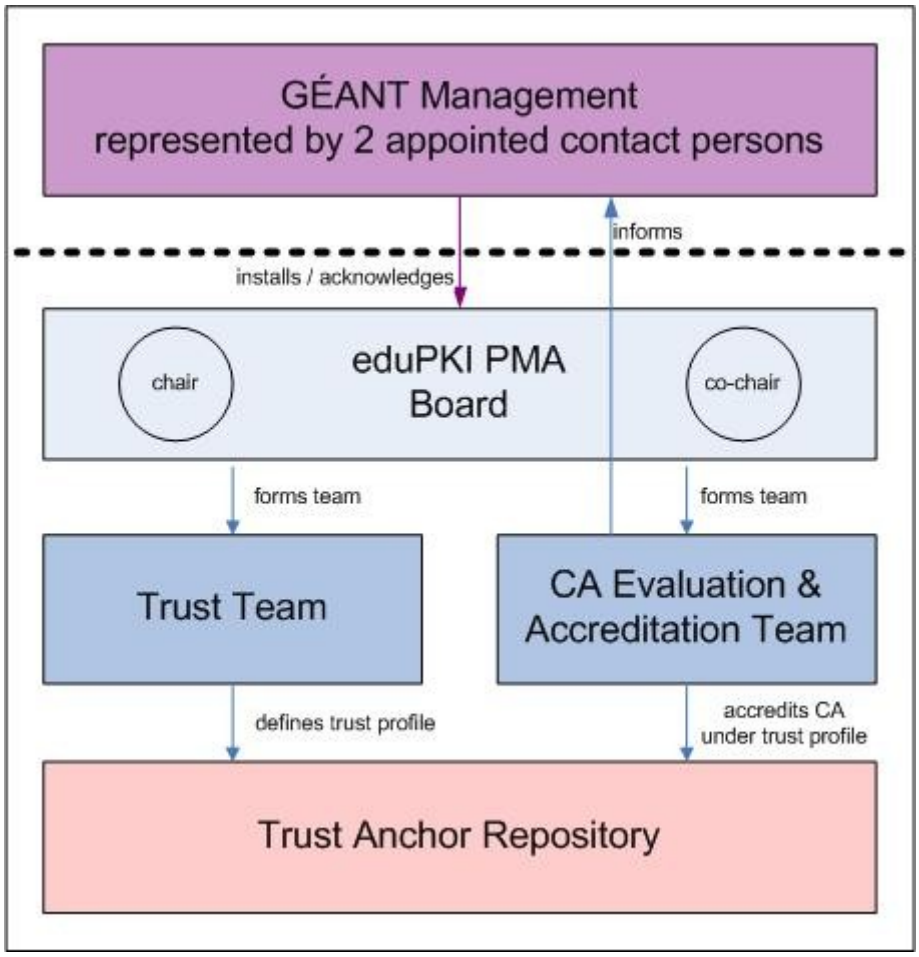

Illustration 1: The eduPKI PMA consisting of two contact persons appointed by GÉANT management, Board, Teams and Trust Anchor Repository;

4.1 eduPKI PMA Board

The Board of the eduPKI PMA consists of individual members which are assigned to work for the eduPKI PMA by their home organizations which must be members of the GÉANT consortium and associated organizations. Within the eduPKI PMA Board the various eduPKI PMA activities are organized in tasks. The eduPKI PMA Board can form and assign Teams to work on specific tasks. The whole eduPKI PMA Board and the eduPKI PMA Teams communicate via electronic means like emails, telephone and video conferences. Under special circumstances face-to-face meetings of the eduPKI PMA Board or Teams may be arranged.

4.2 eduPKI PMA Teams

The following listed Teams and tasks are initially formed. Other Teams and tasks are formed as it's deemed necessary by the Board, e.g. an "Operations Team" to perform any administrative tasks. The Teams may consult with external experts to fulfil their responsibilities.

4.2.1 Trust Team

The "Trust Team" is responsible for gathering requirements from GÉANT Services and other Relying Parties about their trust needs in terms of identity assurance. This Team is further responsible to define and publish a compiled common set of eduPKI Trust Profiles from these requirements which need to be adopted by CAs if they want to become accredited under a

specific eduPKI Trust Profile.

4.2.2 CA Evaluation and Accreditation Team

The "CA Evaluation and Accreditation Team" is responsible to define and publish an evaluation guideline and process to evaluate applying CAs in regards to a chosen eduPKI Trust Profile for eduPKI PMA accreditation under such profile as well as processes to revoke and withdraw such accreditation. The Team performs the evaluation and may guide the applicant through the evaluation process. After successful evaluation of the applicant the Team is accrediting the CA under the evaluated eduPKI Trust Profile. The Team is also responsible to call for and evaluate audit reports of accredited CAs to sustain the level of quality and to take actions if accredited CAs don't match the requirements defined in the eduPKI Trust Profile applicable. Actions can be the timely and coordinated resolution of any open issue, the temporary suspension of the CA's accreditation up to the permanent withdrawal of that CA's accreditation.

4.3 eduPKI Trust Anchor Repository

The eduPKI PMA requires CAs to publish their relevant trust anchors and supplementing information in the eduPKI Trust Anchor Repository before the accreditation process can start. The eduPKI PMA will then announce and publish the accreditation, temporary suspension, or permanent withdrawal of the accreditation of such CAs under the relevant eduPKI Trust Profile in the eduPKI Trust Anchor Repository. The common TERENA Academic CA Repository (TACAR, www.tacar.org), which is also used by other PMAs such as the International Grid Trust Federation (IGTF), is the designated eduPKI Trust Anchor Repository for the eduPKI PMA accredited CAs.

4.4 The GÉANT management

By virtue of the GÉANT management the eduPKI PMA is in charge of defining the trust fabric for all GÉANT Services that have a use for asserted identities based on X.509 digital certificates.

The GÉANT management installs the eduPKI PMA with this Charter and has the final decision on subjects within the eduPKI PMA.

The GÉANT management appoints two contact persons for communication between the eduPKI PMA and the GÉANT management. The appointed contact persons should be well informed about the overall objectives of the eduPKI PMA and have some basic understanding of PKI and trust matters.

The following steps are taken to guarantee a flexible and quick workflow: The eduPKI PMA through its chair will immediately inform the GÉANT management via the appointed contact persons about important decisions, e.g. major changes of this Charter, the accreditation of an applying CA, its temporary suspension or permanent withdrawal. The eduPKI PMA's decisions take immediate effect. In case of objection by the GÉANT management the objected decision is revoked. Due to the careful decision taking process within the eduPKI PMA this is generally not expected to happen.

5 Documents of the eduPKI PMA

The eduPKI PMA develops, publishes and maintains a set of documents listed in this section. Additional documents may be developed and published by the eduPKI PMA as deemed necessary.

5.1 eduPKI PMA Charter

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

5.1.1 Change procedure

The eduPKI PMA Charter document can only be changed following the documented change procedure. Changes must be voted on by the eduPKI PMA's Board (see section 8). For other changes than spelling corrections, clarifications or rewordings final approval must be sought from the GÉANT management (see section 4.4). When changing this document the version number of this document must be increased and section 2 must be adopted accordingly to reflect this change.

5.2 CA accreditation process

The CA Evaluation and Accreditation Team publishes the accreditation process and procedures for PKIs and their CAs in a document called "CA Accreditation Process" [CA-ACC-PROC]. This document describes

- how a CA is obtaining accreditation under a specific eduPKI Trust Profile by getting reviewed by the eduPKI PMA; and
- how a CA is securing its accreditation by adopting changes to the relevant eduPKI Trust Profile and performing audits and delivering audit reports; and
- how an accreditation of an accredited CA is withdrawn.

5.3 GÉANT Services registration process

The Trust Team publishes the registration process and procedures for GÉANT Services in a document called "GÉANT Services Registration Process" [SERV-REG-PROC]. This document describes how a GÉANT Service can register as a Relying Party under one or more eduPKI Trust Profiles.

5.4 eduPKI Trust Profiles

The Trust Team gathers trust fabric 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 *eduPKI Trust Profiles*, represent the different requirements, trust characteristics and identity assertions that GÉANT Services have in regards to their authentication needs.

The Trust Team defines, publishes and maintains one or more common eduPKI Trust Profiles that are acceptable to GÉANT Services. The structure of eduPKI Trust Profiles is described in the "GÉANT Services Registration Process" [SERV-REG-PROC] document.

When changing an eduPKI Trust Profile document its version number must be increased.

eduPKU Trust profile documents must have an uniquely assigned Object Identifier (OID) under an eduPKI Trust Profile specific OID arc including the version number of the eduPKI Trust Profile document.

6 Activities of the eduPKI PMA

The eduPKI PMA will undertake the following activities in the course of its work:

- query the GÉANT Services for their requirements on X.509 PKI identity assertions and certificates (trust requirements),
- define and publish one or more common eduPKI Trust Profiles – based on the GÉANT Services' trust requirements, best practices and standards – each setting minimum criteria to be fulfilled by PKIs' CAs that serve the GÉANT community and in particular GÉANT Services and wish to be accredited under such an eduPKI Trust Profile,
- register new GÉANT Services as Relying Parties for one or more eduPKI Trust Profiles
- maintain a list of registered GÉANT Services and their Relying Parties, which use or want to use the eduPKI Trust Anchor Repository
- evaluate, review and accredit PKIs with their CAs under an eduPKI Trust Profile
- maintain per eduPKI Trust Profile lists of accredited PKIs and CAs
- call for audit reports of the accredited CAs in regards to the eduPKI Trust Profiles the CAs are accredited under and evaluate the audit reports to get detected deficiencies resolved within a set time frame,
- temporarily suspend the accreditation of a CA if any issues compromise the trust into that CA
- permanently withdraw the accreditation of a CA if that CA is not able to resolve deficiencies between its actual operations and the minimal criteria set by the eduPKI Trust Profile it is accredited under in a time frame that the eduPKI PMA has set,
- endorse the use of assured identities within the GÉANT community and their services,
- establish a trust fabric within the GÉANT community,
- publish a set of documents including this Charter document that defines how the eduPKI PMA itself is organized; its members, its membership processes, its chair; how accreditations, decisions and motions are prepared; and how and by whom voting is conducted on these.

6.1 Managing accreditation of CAs

The CA Evaluation and Accreditation Team is managing the accreditation of CAs. Details of the applicable processes and procedures are documented in a separate document listed in section 5.2.

6.1.1 Publishing the accreditation of CAs in the eduPKI Trust Anchor Repository

Once a CA has published its trust anchors at the eduPKI Trust Anchor Repository (see section 4.3) and the CA is successfully accredited under a specific eduPKI Trust Profile in accordance with the eduPKI PMA accreditation process the CA Evaluation and Accreditation Team publishes the accreditation status in regards to the relevant eduPKI Trust Profile of the CA in the eduPKI Trust Anchor Repository. Details of the applicable processes and procedures are documented in a separate document listed in section 5.2.

6.1.2 Publishing the suspension or withdrawal of accreditation of CAs in the eduPKI Trust Anchor Repository

Once an accreditation of a CA is withdrawn or suspended in accordance with the eduPKI PMA accreditation process the CA Evaluation and Accreditation Team removes the accreditation information in regard to the relevant eduPKI Trust Profile from the CA in the eduPKI Trust Anchor Repository. Details of the applicable processes and procedures are documented in a separate document listed in section 5.2.

6.1.3 Removal of trust anchors of CAs from the eduPKI Trust Anchor Repository

If the trust anchors of an accredited CA are not or no longer published in the eduPKI Trust Anchor Repository the accreditation status of the CA cannot be shown and in due course all eduPKI PMA accreditations are withdrawn from the CA.

6.2 Managing registration of GÉANT Services as Relying Parties

The Trust Team is managing the registration of GÉANT Services as Relying Parties. Details of the applicable processes and procedures are documented in a separate document listed in section 5.3.

6.3 Crafting eduPKI Trust Profiles

The Trust Team can decide by vote (see section 8) to introduce a new eduPKI Trust Profile (see section 5.4) if requested by a registered Relying Party or the GÉANT constituency.

6.4 Operations

6.4.1 Registering and holding the eduPKI PMA domains

The domains edupki.net, edupki.org and edupki.eu are registered on behalf of the eduPKI PMA Board of the eduPKI PMA. The domains are used to provide a web server, mail addresses and mailing list services to allow the eduPKI PMA to communicate with its Board members, accredited CAs and registered Relying Parties.

6.4.2 Operating the eduPKI PMA web site

To publish information about the eduPKI PMA and the issued documents the eduPKI PMA will operate a web site under the domains as registered above.

6.4.3 Operating the eduPKI PMA mailing list

Mailing lists will be operated to communicate with external and internal eduPKI PMA groups. The eduPKI PMA will operate one or more specific mailing lists. Depending on the list's purpose access to the list is public or closed and may be restricted to a certain audience.

6.5 Out of scope

The eduPKI PMA will not

- make any explicit or implied authorisation decision for the GÉANT Services (as Relying Parties) and their users,
- issue any identity assertions like X.509 digital certificates itself,

- make any recommendations about user practices.

The eduPKI CA is formally not entangled with the eduPKI PMA. This guarantees that the eduPKI PMA stays neutral in terms of the accreditation of CAs.

7 Membership and participation

The eduPKI PMA comprises the eduPKI PMA Board with its Teams.

7.1 Membership

Members are individual PKI experts, who work in the eduPKI PMA Board by assignment of their NREN which must be a member of the GÉANT consortium. Members must belong to at least one of the Teams working for the Team's task. It is expected from members to participate in their Teams' meetings and other communication necessary to coordinate work in the eduPKI PMA and the Teams.

7.1.1 Type of members

Besides being a regular member of the eduPKI PMA Board working on one or more task Teams there are the positions of the chair and the co-chair of the eduPKI PMA. Chair and co-chair are responsible for

- coordinating and working on the Teams,
- leading and overseeing all external matters and communications and
- leading and overseeing internal matters

of the eduPKI PMA, e.g. organizing and leading video conferences and meetings, coordinating and setting agendas for meetings, releasing information to media and press and communication with the GÉANT management (see section 4.4).

7.2 Membership processes

This section describes who and how an individual becomes a member, chair or co-chair of the eduPKI PMA Board.

7.2.1 Becoming a member of the eduPKI PMA Board

Interested NRENs that are members of the GÉANT consortium can assign PKI experts to join the eduPKI PMA Board and actively work on at least one of the Teams. The existing Board members must accept the assignment by voting (see section 8). The assigning NREN must sponsor the time for the assigned PKI expert who is expected to participate on eduPKI PMA Board meetings, the Team meetings and to work actively on the tasks of the Teams.

7.2.2 Leaving the eduPKI PMA Board

An eduPKI PMA Board member can leave the Board and with that the Teams he/she is associated with at any time, announcing the fact to the chair of the Board. The eduPKI PMA Board may vote (see section 8) a Board member out of the Board if he/she does not actively participate in the Board and Team activities as is expected from his/her role.

7.2.3 Becoming the chair or co-chair of the eduPKI PMA

The position of the chair and co-chair of the eduPKI PMA must be served by an eduPKI PMA Board member. The eduPKI PMA Board is nominating members of the Board for these positions, then voting to confirm them. The terms for chair and co-chair are one year.

7.2.4 Passing the chair or co-chair of the eduPKI PMA

A chair/co-chair can step back from the position he/she serves at any time. After a year of service the term of the chair/co-chair is finished, concluding in the election of a new chair/co-chair. A person can serve more than one term in a row on these positions if voted for by the eduPKI PMA Board.

8 Voting within the Board or a Team of the eduPKI PMA

Voting is done on several items the eduPKI PMA controls:

- changes to this Charter document
- introduction and changes of eduPKI Trust Profiles
- accreditation of CAs and its withdrawal or suspension
- demanding actions to resolve any reported deficiencies in regards to the operation of an accredited CA towards the requirements defined by the eduPKI Trust Profile applicable
- registration of Relying Parties
- accepting members to the eduPKI PMA Board
- dismissing members from the eduPKI PMA Board
- position of the chair and co-chair of the eduPKI PMA

8.1 Availability of a submission to be voted on

The item to be voted on must be available to the eduPKI PMA Board/Team at least two weeks before the vote is taken. In urgent cases, i.e. compromise of a trust anchor or its infrastructure, the eduPKI PMA can decide on immediate actions. In this case the eduPKI PMA must inform the GÉANT management (see section 4.4) immediately about these actions taken.

8.2 Quorum

To have a voting quorum at least three quarters of eduPKI PMA Board/Team members must be present.

8.3 Taking the vote

A decision must be taken by the eduPKI PMA Board/Team if the vote is being conducted open or closed. Valid votes are yes (in favour of the submission), no (against the submission) and neutral (abstention).

8.4 Passing or failing of a submission

The vote passes if at least 51% of the present voting quorum are in favour of the submission. Otherwise it fails.

Glossary

The glossary is available online: https://www.edupki.org/documents/glossary

References

[CA-ACC-PROC] eduPKI PMA, description of the accreditation process and procedures for PKIs and their CAs, "eduPKI PMA CA Accreditation Process", 2010

[GLOSSARY] The Glossary for eduPKI PMA documents. https://www.edupki.org/documents/glossary

[SERV-REG-PROC] eduPKI PMA, description of the registration process and procedures for GÉANT Services, "eduPKI PMA GÉANT Services Registration Process", 2010