Policy Management Authority Charter

for the

DOEGrids PKI

Version 1.6

9/10/2002

1 Introduction

The DOE Grids Certificate Authority was created to support DOE Scientist and Engineers working on the new Computational Grids being deployed around the world. This service issues Identity Certificates to individual subscribers and Service certificates for Grid Services. To manage this Certificate service the DOE Grids PMA has been established. The procedures and guidelines defined in this document specify the roles and responsibilities of the DOE Grids PMA as it pertains to the operation of the DOE Grids Certificate Authority.

The DOE Grids PMA is solely responsible for setting, implementing, and managing certificate policy and practices regarding the DOEGrids PKI.

This charter is based on the Global Grid Forum's working draft: "Policy Management Authority Charter".

2 Scope of PMA

The PMA is responsible for certification and accreditation of the overall PKI implementation and has responsibility for oversight of all PKI operations. The PMA is responsible for the specification and management of the DOE Grids CP/CPS. The PMA is also responsible for the following:

1. Manage PMA membership.
2. Approving and revoking Registration Authorities membership in the PMA
3. Approving and revoking certificates of Registration Authorities and/or their Agents
4. Approving and revoking deployment of remote Registration Managers. To include: Site specification, Access control and Agent responsibilities.
5. Ensuring appropriate use of PKI facilities throughout the DOE Grids PKI
6. Report Annually to the ESSC. (Pending acceptance by the ESSC)
7. Publishing all related documents.
8. Schedule meetings of the PMA and publishing meeting minutes.

The PMA is the point of contact for: Relying parties and subscribers in the PKI. Relying parties can contact the PMA to raise issues like: new applications, certificate usages, certificate roles, re-registration, security concerns, etc.

The PMA is also the point of contact for: other PKI PMA's, potential new members or relying parties.

3 PMA Membership

3.1 Creation of PMA

The initial DOE Grids PMA will consist of:

1. ESnet staff members responsible for the deployment of the service – ex official members.
2. DOE Science Grid leads responsible for Grid PKI services.
3. A member from the Globus software Project
4. A member from each of the founding Registration Authorities.

3.2 New Members

It is assumed that the PMA will add new members over time. New Virtual Organizations or Sites will be added to the service. It is expected that each new site or VO will appoint a point of contact for that user community. This POC will have the additional responsibility of representing their community by becoming a member of the PMA.

As part of the process of approving the new VO or Site, the PMA must also approve the Sites POC as a new member of the PMA.

3.3 Type of Membership

3.3.1 General membership

The DOEGrids PMA membership is based on constituent organizations, but is made up of named individuals. The active list of PMA membership is found on the service website: http://www.doegrids.org/pages/doegridspma.htm
Each new Member to the PMA requires an official introduction ceremony. At this ceremony the DOE Grids Security officer [1]reviews, with the new applicant the policy and procedures that each new RA or CA manager is responsible for.

3.3.2 Ex officio membership

The ex officio memberships are full voting members of the PMA. These members are drawn from the community at large and may not represent a constituent organization or the registration authority for that organization. Possible sources are: ESnet operations, Middle ware providers (i.e. Globus) or scientific leads in the community. All ex officio members are nominated and approved by the PMA.

3.3.3 PMA chair

The PMA will elect a chair to manage the PMA. This position is to be filled from the membership of the PMA. The term as chair is to be one year. The chair may resign by written request to the PMA. The PMA, by vote can remove the Chair. The chair is responsible for:

1. Point of contact for the PMA
2. Liaison to ESnet operations
3. Running the PMA meetings
4. Insuring Minutes are taken and published.
5. Insuring that all voting is recorded and published

[1] The DOE Grids Security Officer is the person Responsible for the Operations and system administration of the PKI software used to provide the DOE Grids PKI. This person is a member of the ESnet staff.

3.4 Membership Guidelines

Participating members should be drawn from a wide range of community members. In particular, members with significant management experience, capable of acting (voting) on behalf of their organization, are desirable.

3.5 Executive Council

If the PMA membership grows too large to be effective in managing the PKI service, it is recommended that the PMA form an Executive council. The Executive Council will be responsible for the management of the PMA.

Membership of the council will be selected from the general PMA membership and installed by vote of the general PMA. The scope of the Executive council will be the management of the full PMA. The full PMA maintains all its responsibilities as outlined in this document and the CP/CPS.

3.6 Withdrawal/Expulsion

Virtual Organizations or Sites may have to end their relationship with the DOE Grids PKI. A VO/Site can withdraw from membership by submitting a written request. This request must be approved by the PMA. The request to withdraw must include how the VO/Site's certificates issued to its subscribers and Grid services are to be dealt with (i.e. Revoked, allowed to expire).

The PMA may decide that a VO/Site should be expelled from the PKI service. This action requires PMA approval.

4 Responsibilities

4.1 CP/CPS

The DOE Grids PMA is responsible for the development and maintenance of the DOE Grids CP/CPS. Maintenance/Revision of the CP/CPS is an on going process. Revisions will be required to keep pace with the development of Grid technologies.

4.2 Other documents

The PMA is responsible for this charter and should add or change this document to deal with changing conditions and membership.

4.3 Audit

The PMA is responsible for assuring that the DOE Grids PKI service is operated in accordance with our CP/CPS and other approved operational documents. The PMA must decide how and when compliance audits are to be carried out for: the DOE Grids CA, its registration authority operations and subordinate CA's.

4.4 Operations

ESnet, funded by the MICS program of DOE, is responsible for the day to day operation of all hardware, software and support infrastructure of the DOE Grids PKI. ESnet provides the staffing, equipment and data center resources required to operate the DOE Grids PKI.

The PMA is responsible for maintaining this relationship. The CP/CPS will constitute the technical portion of the contract between the PMA and ESnet.

4.4.1 ESnet PKI Management

ESnet staffs and operates the DOE Grids PKI on a day-to-day basis and assures that it is functioning properly, that all procedures and safeguards are being followed, and that any operational errors, anomalies, breeches of security or policy, and/or procedure are addressed promptly and properly. Because the PKI itself is a trust-oriented service, it is essential that ESnet institute, and consistently follow, operational procedures that promote reliability and trust.

4.4.2 ESnet PKI Management Responsibilities

ESnet staffs and operates the Certification Authority (CA) server and its associated directories, repositories and communication facilities. ESnet is responsible for developing and maintaining PKI plans, policies and procedures pertaining to operation of the Certification Authority and the overall operation of the PKI. This includes:

- Implementing the policies and directives of the Policy Management Authority
- Access control of the CA server
- Information security for the PKI
- Staffing and assignment of duties for PKI personnel
- PKI staff training
- Development of CA's operating procedures
- Liaison with vendors
- Operating and maintaining the CA server
- Operating and maintaining the LDAP directory
- Maintaining official CA records and activity logs
- Evaluating new technology
- Maintaining and refreshing existing technology
- Disaster recovery procedures

4.4.3 ESnet PKI Management Routine Activity

ESnet provides availability of the Certification Authority and its associated Directory on a 24 hours/day, 7 days/week basis.

ESnet PKI Management staff will:

- Issue Certificate Revocation Lists (CRLs)
- Verify the physical security and integrity of the CA server facility
- Receive new hardware and software
- Produce and store backup copies of Certification Authority database and journals
- Review adequacy of PKI configuration and recommend improvements if necessary.
- Review adequacy of PKI procedures and make improvements as necessary
- Test (and replace where necessary) archival files
- Immediately report security, processing, or procedural anomalies or violations to the PMA.

4.4.4 Procedural Requirements

ESnet will establish and publish detailed procedures for all aspects of the Certification Authority operations. The procedure documentation and its associated records will be sufficient to permit verification by independent auditors that ESnet is fully compliant with the policies and directives of the Policy Management Authority. At a minimum, ESnet's procedure set will encompass the following subjects:

- Routine Certification Authority server procedures
- Key Recovery procedures for the CA
- Disaster Recovery procedures
- Backup for the Subscriber's public certificates.

4.5 Directory

X.509 certificate services have hidden or explicit dependencies on directory (LDAP, X.500). The PMA is responsible for providing direction for the operation of the DOE Grids directory.

5 Activities

5.1 Point of Contact

The PMA is responsible for publishing to the DOE Grids website the PMA membership and contact information. http://www.doegrids.org/pages/doesgpma.htm.

5.2 Meetings

The PMA will meet periodically (as described in the by-laws). The PMA must provide the ability for members to conference remotely, such as by telephone conference, H.323, Access Grid.

Agendas will be posted by the chairman in advance of these meetings. Minutes will be posted by the chairman and maintained in an archive for 10 years.

6 Bylaws

6.1 Intro

This section describes the rules for specific requirements the PMA must carry out as part of the DOE Grids PKI service. It lists a number of areas of responsibilities and the procedures for carrying out those duties.

6.2 DOE Grid PKI membership requests

A Virtual Organization or Site can apply for membership in the DOE Grids PKI service, by submitting a written request to the PMA. When the PMA receives an applications from a Virtual Organization or Site to run a RA as part of the DOEGrids PKI the PMA must:

1. Validate the Virtual organization or Sites' identity.
2. Validate the identity of the Point of Contact – RA.
3. Validate that the RA represents the VO or Site.
4. Validate the identity of any Agents working for the RA.
5. Approve the RA operational procedures (appendix to CP/CPS)
6. Direct the DOEGrids Security officer to issue Agent certificates to the new RA/agents.

6.2.1 Validating VO or Site identity

The PMA must determine the legal existence of the VO or Site. Sties have a physical presents and a history in the community that can be easily documented by DOE Headquarters. VO's require proof of existence; this can be done by checking with DOE Headquarters to determine if they have funded or created the VO. VO outside DOE will require the funding agency to validate the existence and mission of the VO.

6.2.2 Validating POC, RA identity

A new member of the PMA must prove their identity. This proof can take the form of Government ID and or sponsorship by another member of the PMA. Every new member must meet with the DOE Grids Security officer before being issued an RA agent certificate. This meeting can be face to face or over the phone if other members of the PMA have met face to face with the candidate.

6.2.3 Validating RA represents the VO or Site

Each new member of the PMA must provide evidence that they are representing their VO/Site to the PMA. They must provide evidence that they can issue to their community DOE Grids certificates and these certificates represent a valid ID for their users.

6.2.4 Validate any agents representing the RA

RA's may decide to delegate to other members of their organization the role/responsibility to validate certificate requests in their community. Each of these Agents of the RA must be identified and meet with the DOE Grids Security officer before agent certificates are issued to them.

6.2.5 Approve the RA operational procedures

Each new Virtual Organization/Site must submit to the PMA an appendix to the DOE Grids CP/CPS that documents their Identity vetting rules. This appendix describes how the RA will operate. The PMA must review and approve this appendix before the RA becomes a member of the PMA.

6.3 PMA meetings

The DOE Grids PMA meets as required, to conduct routine business at a time and place announced by the Chair. An agenda is prepared in advance and distributed by the chair. The meeting can be at a physical site or conducted with Audio or Video conferencing. Typically the agenda will include the following items:

- Staffing changes within the PKI Operations
- Applications for membership to PMA or the PKI service.
- Pending changes to policies or other PKI management directives
- Review of PKI-related procedures and record-keeping practices
- Review matters of consideration presented by ESnet PKI participants
- Changes to the PKI configuration (hardware, software, location, etc.)
- Proposed and pending enhancements and expansions.
- Incidents and non-routine events
- Interfaces with other organizations
- Changes in standards or technology.

Minutes of each meeting must be taken and archived. The minutes must be approved by the PMA.

6.4 PMA approval process

PMA approval is arrived at by either obvious consensus as determined by the chair or by a vote. When the PMA must vote to fulfill it obligations, that vote will be made by a quorum of the PMA members. A quorum is defined as more then 50% of the current PMA membership. A positive vote will be recorded if more then 50% of the voting quorum votes in favor of the proposal. The vote must be carried out at an official meeting of the PMA. The proposal and its associated vote will be recorded in the minutes of the meeting. These minutes will be the official record of the voting process. The vote can also, occur over email, with the mail archive acting as the official record. If the vote is to be over email the voting period will be a minimum of 10 working days.

7 Security

The PMA has no security issues of its own. The PMA may decide that operational and audit information may need to be limited to a select audience.