# Policy Management Authority Charter

# for the

# DOEGrids PKI

## Version 1.7

## 5/23/2005

Tony J Genovese
503605

Digitally signed by Tony J Genovese 503605
DN: CN = Tony J Genovese 503605, OU = People
Reason: I attest to the accuracy and integrity of this document
Date: 2006.01.13 14:50:00 -08'00'

# Table of Contents

# 1 Introduction

The DOE Grids PKI was created to support DOE scientist, engineers and their colleagues working the computational Grids being deployed around the world. This service issues Identity Certificates to individual subscribers and Service certificates for Grid services. To manage this PKI 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 PKI.

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 “Policy Management Authority Charter”.

# 2 Scope of DOEGrids 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. Approval or removal of Registration Authorities to the PMA board
3. Approval or revocation of certificates issued to Registration Authorities and/or their Agents.
4. Ensure appropriate use of the DOE Grids PKI
5. Publish all related documents.
6. Schedule regular meetings of the PMA and publishing meeting minutes.

The DOEGrids PMA is the point of contact for:

1. All DOEGrids relying parties and subscribers in the PKI.
2. Peering PMAs like: The Americas Grid PMA, EU Grid PMA and the AP Grid PMA.
3. Potential new members or relying parties

# 3 DOEGrids PMA Membership

The active list of PMA membership is found on the service website: http://www.doegrids.org/pages/doegridspma.htm

## *3.1 Creation of PMA*

The initial DOEGrids PMA was set up September 10, 2002 when version 1.6 of the PMA charter was accepted by voice vote of the founding members. The founding members consisted of:

1. ESnet staff members responsible for the deployment of the service.
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 Membership types*

The DOEGrids PMA will consist of members drawn from our user community. As grids are being deployed today they are crossing physical or logical site bounties. A unit of organization that is common in the Grid community is the Virtual Organization. This loosely leaves us as defining our user community as consisting of the following:

1. Virtual Organizations (VO)
2. Large sites in the DOE community
3. Universities
4. Other organizations approved by DOE Office of Science that support DOE research projects or staff.

The DOEGrids PMA will consist of people having the following community roles:

1. **DOEGrids Registration Authorities:** They are members that are directly responsible for the management of the DOEGrids PKI for a specific Virtual Organization or Site. These members will be responsible for the Registration Authority operations and customer support for their VO/Site. They must be capable of voting on behalf of their organization and user community.
2. **Relying parties:** They represent communities that depend on the trust worthiness of DOEGrids certificates. They are full voting members of the board.
3. **Ex officio members:** They are drawn from the general community. These members are not responsible for running an RA. They will be advisors to the board on issues that affect the deployment or acceptance of the service by the community. They are full voting members of the board.

## *3.3 New or renewing Members*

The PMA will add new members over time. New Virtual Organizations (VO) or Sites will be added to the service. Each new site or VO will appoint a point of contact for that user community. This POC will have the responsibility of representing their community by becoming a voting 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.

The term of membership for all PMA board members will be for one year. Renewal of membership will occur at the annual meeting of the PMA. Each member of the PMA that is also a new or renewing Registration Authority must also send a digitally signed email to the DOEGrids PMA which includes the RA declaration letter as outlined in Appendix A of the DOEGrids CP/CPS.

Each new candidate for the PMA requires an official introduction ceremony. At this ceremony the DOEGrids Security Officer reviews, with the new applicant the policy and procedures that each new RA is responsible for. A review of the VO or Site appendix is covered with the new candidate. This introduction ceremony must be done face to face or the sponsoring member of the DOEGrids PMA will need to verify the identity of the individual. After this introduction/review the DOEGrids Security Officer will direct the DOEGrids operations staff to authorize the new RA's certificate for RA access.

## *3.4 DOEGrids PMA officers*

The DOEGrids PMA will be organized as a permanent society consisting of the following officers and roles:

1. Chairperson
2. Secretary
3. Security officer
4. General membership, RAs
5. Ex officio membership

The election of PMA officers will occur at the annual meeting of the PMA. Voting will be done by the new and renewed members.

### 3.4.1 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

### 3.4.2 Secretary

The PMA will elect a secretary which will have a term of one year. The secretary may resign by written request to the PMA. The PMA, by vote can remove the secretary. The Secretary will have responsibility for:

1. Maintaining the official minutes of the PMA meetings.
2. Manage the PMA's email archive and document repository.
3. Manage the email list membership.
4. Coordinate editing and publishing of all PMA documents.

### 3.4.3 Security Officer

The PMA will elect a Security Officer which will have a term of one year. The Security Officer may resign by written request to the PMA. The PMA, by vote can remove the Security Officer. The Security Officer will have the responsibility for:

1. POC for any security question sent to the PMA board.
2. Oversight of the standing Security incident handling committee.

3. Liaison to the ESnet PKI operations staff

### 3.4.4 Liaison Officers

DOEGrids needs to coordinate its efforts with external organizations involved with PKI or relying on our authentication system. DOEGrids Liaisons will be responsible for maintaining communications between our group and external groups.

The PMA is responsible for specifying with which groups they wish to coordinate. It is the responsibility of the Chair of the PMA to appoint official DOEGrids Liaisons. The appointment is for one year and can be renewed as deemed by the PMA.

## *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 acknowledged 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 DOEGrids PMA 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 any subordinate CA's.

## *4.4 DOEGrids PKI 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.

## *4.6 Security Incident committee*

The Security incident committee is a standing committee of the PMA. The PMA Security Officer will chair the committee. At least two other volunteers from the general PMA membership and ESnet DOEGrids Operations staff will work on the committee. This committee is to handle security issues that are presented to the PMA. They will advise the PMA on what should be done to close the security incident.

### *4.7 DOEGrids document committee*

The DOEGrids PMA will maintain a standing committee to review and edit the documents used by the PMA. This committee will be chaired by the Secretary and will include at least two volunteers. They will be responsible for advising the PMA on required changes or updates to the PMA documents.

# 5 DOEGrids Governance

## *5.1 Introduction*

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.

## *5.2 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

## *5.3 DOE Grid PKI membership requests*

There are two types of membership requests. The first is a membership that has the responsibility for operating a Registration Authority. The other is the Ex Official class of member. Each membership requires different processing.

### 5.3.1 Registration Authority Membership

A Virtual Organization or Site can apply for membership in the DOE Grids PKI service if they meet the membership requirements in subsection 3.2. They would apply for membership by submitting a written request to the PMA. When the PMA receives a request from a Virtual Organization or Site to run a RA as part of the DOEGrids PKI the PMA must first find a member of the board that will act as a sponsor for the new candidate. If no sponsor on the board is found the request for membership will be rejected. This sponsor will be responsible for representing the candidate before the board and reporting back to the PMA concerning:

1. Validation of the Virtual organization or Sites' identity.
2. Validation of 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. Review the RA operational procedures (appendix to CP/CPS) for compliance to our policies
6. Make a recommendation to the board regarding acceptance or rejection of membership request.
7. If membership is approved the board will Direct the DOEGrids Security officer to issue Agent certificates to the new RA/agents.

### 5.3.1.1 Validating VO or Site identity

The sponsor of the new member will help the PMA in determining the legal existence of the VO or Site. Sties have a physical presence 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.

### 5.3.1.2 Validating POC, RA identity

The sponsor will work with the new candidate to provide proof of their identity to the PMA. 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.

### 5.3.1.3 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.

### 5.3.1.4 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 formally introduced to the DOE Grids Security officer before the Security officer will direct PKI operations to grant agent status to them.

The formal introduction will be accomplished by the RA by sending a signed email to the Security officer identifying his/her new Agent. The new Agent must send a signed Agent Declaration email to the Security officer and PKI operations according to the rules and template outlined in Appendix A of the DOEGrids CP/CPS.

### 5.3.1.5 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.

### 5.3.2 Ex Official Membership

Ex Official members are drawn from the general community. These members are not responsible for running an RA. They will be advisors to the board on issues

that affect the deployment or acceptance of the service by the community. They are full voting members of the board.

An individual can be sponsored as an Ex Official member by any member of the DOEGrids PMA. This sponsor will be responsible for representing the candidate before the board and to report back to the PMA concerning:

1. That the candidate provides expertise that affect the deployment or acceptance of the service by the community
2. Proof of the individual's identity.

## *5.4 PMA meetings*

The DOE Grids PMA meets quarterly or as required, to conduct routine business at a time and place announced by the Chair. The annual meeting of the PMA will occur during the 3rd calendar quarter. This meeting is mandatory and will conduct the annual election of officers. 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 will be posted by the secretary and maintained in an archive for 10 years.

## *5.5 Officer elections*

The DOEGrids PMA officers will be elected by the PMA at the annual meeting, subsequent to the renewal of existing members and approval of new members. Nominations for office can come from an individual volunteering or from any member on the board. The election will follow the normal PMA approval process. If multiple members are running for the same position, the candidate with the most votes will win.

## *5.6 PMA voting 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 than 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 may 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 and a maximum of 15 working days.

# 6 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.

# 7 Change log

| Version | Date | Changes |
|---|---|---|
| 1.0 – 1.6 | Sep 10 2002 | Creation of the DOEGrids from DOE Science Grid PMA |
| 1.7 | April 30, 2005 | 1. Modified Scope to add peering and POC relationships<br>2. Mod Membership to define new roles: Chair, Secretary, Security officer.<br>3. Added Security committee 4.6<br>4. Modified meetings to be quarterly.<br>5. **removed PMA approval for member resignation**<br>6. **added guidance on Agent process in 6.2.4**<br>**7. Added max time limit on voting.**<br>**8. Modified the Membership types and added Relying parties**<br>**9. Modified membership procedures**<br>**10. Added official Liaison role**<br>**11. Added officer elections**<br>12. **Added standing** |

| | | |
|---|---|---|
| | | **editing committee** |