Procedures and guidelines for the Policy Management Authority of the ESnet PKI

Version X.X - DRAFT

5/16/2002

Introduction

ESnet has established a Public Key Infrastructure to support its user community. The ESnet Root Certificate Authority has signed the DOE Science Grid subordinate Certificate Authority. These procedures and guidelines define the operation of the ESnet PMA that has oversight for the DOESG Certificate Authority.

The PMA is responsible for setting, implementing, and managing certificate policy and practices regarding the ESnet PKI.

1 Responsibilities

The PMA is responsible for certification and accreditation of the overall PKI implementation and has responsibility for oversight of all PKI operations. The PKI Policy Management Authority is also responsible for the following:

1. Approving and revoking Registration Authorities membership in the PMA
2. Approving and revoking certificates of Registration Authorities and/or their Agents
3. Approving and revoking deployment of remote Registration Managers. To include: Site specification, Access control and Agent responsibilities.
4. Ensuring appropriate use of PKI facilities throughout the ESnet PKI
5. Maintaining and publishing the Certificate Policy and Certification Practice Statement.
6. Oversight of PKI policies
7. Review Certification Authority operations and activity
8. All technical, hardware and software aspects of the PKI
9. The PKI Policy Management Authority may commission audits of PKI operations.
10. Report Annually to the ESSC. (Pending acceptance by the ESSC)

Formatted: Bullets and Numbering

Deleted: operations

Formatted: Highlight

Formatted: Font: (Default) Times New Roman

2 PMA Routine Activity

The ESnet PMA meets quarterly, or 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
- 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.

Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial

3 Procedural Requirements

The ESnet PKI PMA will adopt and publish procedures it may deem necessary to discharge its responsibilities and conduct its business efficiently. The official email address of the PMA is pma@es.net. The official Web site for the ESnet PKI service is: www.DOEGrids.org. All service related documents and information will be posted to this site.

3.1 Approval process

When it is deemed necessary that 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 can only 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.

3.2 PMA membership

Formatted: Heading 2

The initial PMA consists of a set of volunteers made up of the project members and the Registration Authorities for the Sites and Virtual Organizations. The official list of PMA members will be maintained on the PKI service web site at:

Formatted: Font: (Default) Arial
Formatted: Indent: Left: 0.04"

http://www.doegrids.org/pages/doesgpma.htm

Formatted: Indent: Left: 0.3"
Formatted: Font: (Default) Arial

Each member of the PMA must be able to commit to membership for at least one year. Any member may resign from the PMA by written notice. If the member is a Registration Authority or a subordinate CA manager for a site or VO they must:

1. Nominate a replacement to the PMA
2. Get PMA approval for the replacement and resignation

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.29" + Tab after: 0.54" + Indent at: 0.54"

The PMA is run as a formal committee. These meetings are called and run by the Chair. The Chair of the PMA is elected by the general body and has a term of one year. This election is to occur at SOME DATE each year. The Chair may resign earlier then his full term with the approval of the PMA

Formatted: Font: (Default) Arial
Formatted: Highlight

4 Reporting and Record Keeping Requirements

The PKI PMA will maintain such records as necessary to support its activities and reporting responsibilities to the ESSC.

Deleted: .

5 ESnet PKI Management

ESnet staffs and operates the ESnet 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.

5.1 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

5.2 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.

5.3 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.

Formatted: Bullets and Numbering