GWD-C
Category: Community Practice Documents
CA Operations WG

Robert Cowles, SLAC
Tony Genovese, ESnet/LBNL

Peter Gietz, DAASI
Michael Helm, ESnet/LBNL
May, 2005

Policy Management Authority Model Charter

Status of this Memo

This memo provides information to the Grid community on constructing a charter for a Policy Management Authority. It does not define any standards or technical recommendations. Distribution is unlimited.

Copyright Notice

Abstract

This document provides a template that can be use to develop a charter for a Grid Policy Management Authority [GPMA] The GPMA is responsible for the management of a “Grid Public Key Infrastructure” [GPKI] and its associated “Grid Certificate Authorities” [GCA]. GPMAs will serve as the points of contact for GPKIs that wish to interoperate. A GPMA is responsible for managing external relationships and any resulting internal changes.

rdc@SLAC.Stanford.EDU et al.

Table of Contents

1 Overview

This is a template for a charter for a Grid Policy Management Authority [GPMA]. A GPMA is responsible for the management of a "Grid Public Key Infrastructure" [GPKI] and it's associated "Grid Certificate Authorities" [GCA]. A GPKI may consist of a single CA [GCA] with one or more points of registration; a bridge between multiple root CAs; lists of acceptable CAs; or other combinations. Since the Grid consists of many different kinds of organizations working towards interoperability, it is reasonable that many GPKIs will exist.

There are already several substantial Grid collaborations that have agreed to work together to manage PKI policies in order that their members can make full use of available resources across these collaborations, and it is expected that there will be many more. These collaborations can also be expected to collaborate with each other at times. A common organizational structure and set of expectations will substantially benefit the various grids. The GPMAs will serve as points of contact for different Virtual Organization's (VO's) and GPKI's that wish to interoperate, and provide a medium for discussing and normalizing policy differences between different organizations. The GPMA will manage external relationships and resulting internal changes (or vice versa), reflecting these changes in its CP and CPS document set.

This document focuses on the current model and issues of using PKI for managing Grid Identities. In the future there could be other technologies that will be used to provide Grid Identities. Any Grid organization or multi-site/VO structure that needs a formal process can make use of this model charter.

The following sections describe or give examples for the content of the GPMA charter. Each section below corresponds to a section in the GPMA charter. Throughout this document the examples are based on a GPKI. Appendix A contains a blank template of a sample GPMA charter. Appendix B contains examples of current use of a GPMA charter.

2 Introduction

In the introduction section you should describe who you are and the community that will be served by the GPMA.

3 Scope

The Scope section will cover the boundary conditions for the GPMA. It will address the question of what is and is not covered by the PMA. For GPKI's the following should be included:

The GPMA's primary responsibility is to manage the CP/CPS documents. This may be a single composite document; or the CP may exist as a template or specification and the CPS as a point-by-point detailed response; or these may be broken up into many separate documents.

The GPMA provides points of contact for insiders – relying parties and subscribers in its PKI. Relying parties in particular need a forum to raise issues: new applications or certificate usages, certificate roles, re-registration, security concerns, etc. The GPMA provides points of contact for external entities such as another PKI PMAs, potential new members, or relying parties. The CP/CPS should provide contact information for the GPMA managing it.

3.1 Included PMA activities

In all cases the GPMA provides access to

- GCA CP and CPS
- Other related documents (Subscriber and End-Entity agreements, auditing reports, white papers)
- Meeting schedules and minutes
- Telephone and email points of contact

3.2 Excluded PMA activities

Specify which items are excluded from review or ownership of the GPMA.

For example, the following might be excluded from oversight in a typical GPMA:

- The definition or enforcements of access policies and practices (authorization)
- The definition of policies and practices for long-term data encryption
- The definition of policies and practices for the use of identity assertions in any financial transaction or transaction having an explicit monetary value

4 Creation of PMA

4.1 Initial membership

Setting up a PMA requires a bootstrapping process. One of the first acts of the PMA would be to vote on its charter. In this section describe how to initialize the PMA and define its membership.

Members of one or more virtual organizations [VOs] running CAs or in need of CA services may agree to cooperate on an interoperable PKI. These VOs appoint an interim chairman (by consensus). The initial set of members will add bylaws to the GPMA charter to manage the question of:

- Charter approval/amendment process
- Adding and removing new members
- Other issues pertaining to the management of the PKI

The initial set of members will set up a hosting organization and web site to provide access to the document set and contact information, and they will appoint a committee to draft the CP and CPS documents. All CAs providing services for the GPKI agree to comply with the terms of the CP and CPS documents and provisions of the GPMA charter.

5 Membership

The GPMA has to be able to manage its members. This section attempts to answer questions like: How does one join the GPMA? What constitutes or defines membership criteria?

5.1 Membership Guidelines

5.1.1 New Member Organizations

It is assumed that the GPKI will add organizations that will operate their own CAs, or their own registration and identity management infrastructures in the GPKI. New member organizations are approved by existing members of the GPMA through a process specified in the bylaws.

New member organizations must agree to abide by the GPMA charter, the CP/CPS and other documents managed by the GPMA; and they must have individuals willing to serve in the GPMA as participating members (see below).

5.1.2 Type of Membership

GPMA membership is based on constituent organizations, but is made up of named individuals from those organizations. A member organization can provide multiple members, so long as it is to the benefit of the GPMA, but number of participating members should not affect the number of votes the member organization is entitled to cast.

5.1.3 Participating Member 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. The bylaws may provide for a ceremony to introduce new participating individuals.

5.2 Executive Council

If the numbers of organizations or additional memberships grows substantially, it will become necessary to split the membership. The membership should select a small body to manage the GPMA.

5.3 Withdrawal/Expulsion

5.3.1 Organizations

Organizations may cease to exist or drastically change their management. The GPMA bylaws should allow for withdrawal or expulsion in these cases.

5.3.2 Individuals

Individual participating members may change roles or may no longer be capable of performing duties on or for the PMA. Member organizations and the PMA bylaws must take these possibilities into account and provide for a means to remove individuals when necessary; allow for a resignation procedure; and a succession mechanism.

6 Responsibilities

This section addresses the primary areas for which the GPMA must be responsible. These include the primary or controlling document set (CP/CPS for GPKI), auditing, operations (CA management), and publishing (X.500 or LDAP directory for current GPKIs). Some of these topics are not yet well developed in GPKI's and so development is left to the PMA. In the case of a GPKI based system the controlling documents are its CP/CPS and related PKI documents. Other identity based systems will have their own controlling document set. The issue of Audits is lightly addressed for this community. Most participating CAs and even PMAs must address the issue. This is important to build trust in your community. Each community must define its needs/requirements for building trust in the Identity provider.

Finally, how the GPMA will manage or interact with the physical provider or operator of identity tokens (X.509 in PKI) has to be addressed.

6.1 CP/CPS

These complex documents require on-going revision and examination. The documents often have "bugs" – errors of fact or errors in specification – that need to be corrected.

The Grid and its software base are undergoing rapid development. The following areas may require adjustment in policies and deployment in the near future:

- CRL and certificate validation infrastructure
- Authority Information extensions
- Key sizes
- Special purpose servers and web services
- Certificate profiles and extensions

6.2 Other documents

The GPMA manages its own charter, and should add or change by-laws to deal with changing conditions and membership. The GPMA may manage documents such as:

- Subscriber (end-entity) and relying party agreements.
- PKI Disclosure Statements
- Operations guides – access to these may be controlled due to security considerations.
- List of participating CA's with contact data.
- Audit reports

6.3 Audit

The GPMA is responsible for assuring that the GCA and GPKI are operated in accordance with the CP/CPS and other operations documents. The GPMA will conduct periodic compliance audits of the GCA, its registration authority operations, and subordinate or component CA's.

The GPMA may hire auditors at various times, as required by the CP, as specified in the by-laws, or as the GPMA sees fit.

The GPMA should publish substantial portions of the audit report.

6.4 Operations

The constituent organizations will hire a CA operator, and may pool resources to create the GPKI. The GPMA is responsible for maintaining this relationship. The CP should constitute the substantive technical portion of the contract with the constituent organizations. The GPMA will manage the contract with the CA operator.

The GPMA is a policy management authority, not an operations unit. It does not manage day-to-day activity of members, the CA operator, or RA operators.

6.5 Directory

In Grid PKI based identity services X.509 certificate services have implicit and explicit dependencies on directory (LDAP, X.500). A GPMA that uses PKI should include directory management and access as part of its GPKI operations. Participating directories should support the same certificate retrieval mechanisms, which are being defined in the IETF pkix WG.

7 Activities

7.1 Point of Contact

The GPMA creates a web site, contact forms, contact postal and email addresses, in its initiation phase. These points of contact should be open to anyone in the community; in the GPKI this is effectively the world.

7.2 Meetings

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

Agendas will be posted by the chairman in advance of these meetings.

Minutes will be posted by the chairman.

7.3 Research

It is expected that Grid requirements and PKI technology will change considerably in the future. The GPMA should support a research committee.

7.4 Decision – making process

The GPMA needs to provide an orderly decision-making process. The GPMA will need to make decisions about amendments to the CP and related documents; to its by-laws; to its schedule; and its membership.

Questions concerning membership, meeting schedule, and by-laws are probably only open to GPMA members for introduction. It may be useful to allow the PKI community or even interested outsiders to introduce amendments to the CP/CPS and related documents.

Questions and amendments submission could be managed by mailing list (perhaps an open- and closed- mailing list to cover open and restricted questions), or by other means as described in the by-laws. The GPMA should set aside a review period for all items under consideration, to allow all parties time to understand the issues.

The GPMA will establish a decision-making system. Consensus works best in some situations and is probably the best way of ensuring trust, but may not scale to a large organization with many members. A majority-vote system has many benefits. The GPMA may choose to establish some other system in its by-laws.

In some cases conflicts may arise that cannot be settled internally. If the GPMA is affiliated with a larger organization, then the by-laws should establish an appeal process.

8 Bylaws

The GPMA may wish to note specific changes to PMA policies listed elsewhere in this document, by referring to section number and listing the change. Bylaws take precedence over other sections of this document.

9 Security

The GPMA has no security issues of its own. Operations guides may need to be limited to a select audience. Audit reports may need to be kept confidential. Both reveal the details of internal operations, and have the potential to identify significant weaknesses. On the other hand, the more open the process is, the

Appendix A Charter template

This section is a blank template with all the section described in the body of the document. It should be modified as appropriate by the organization using it.

1 Introduction

2 Background

3 Scope of the PMA

3.1 Included activities:

3.2 Excluded activities:

4 Creation of PMA

4.1 Initial Membership

5 Membership

5.1 Membership Guidelines

5.1.1 New Member Organizations

5.1.2 Type of Membership

5.1.3 Participating Member Guidelines

5.2 Executive Council

5.3 Withdrawal/Expulsion

5.3.1 Organizations

5.3.2 Individuals

6 Responsibilities

6.1 CP/CPS

6.2 Other Documents

6.3 Audit

6.4 Operations

6.5 Directory

7 Activities

7.1 Point of Contact

7.2 Meetings

7.3 Research

7.4 Decision – making process

8 Bylaws

9 Security

Appendix B Examples

ESnet – DOE Grids PKI

http://www.doegrids.org

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

This GPMA is made up of several constituent organizations, and is operated by ESnet. The GPMA charter document is still being developed. Its current practices influenced this GPMA document.

EU Grid PMA

The EUGridPMA is currently being established as a successor to the Certification Authority Coordination Group (CACG) that was established by the European

DataGrid project and used as well by CrossGrid and the LHC Computing Grid projects.

http://www.eugridpma.org/

US Federal Bridge

http://www.cio.gov/fpkipa/

Policy Authority charter: http://www.cio.gov/fpkipa/documents/fpkipa_charter.pdf

This PKI's set of bylaws has influenced the ESnet PKI

Glossary

None

Intellectual Property Statement

The GGF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the GGF Secretariat.

The GGF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this recommendation. Please address the information to the GGF Executive Director.

Full Copyright Notice

rdc@SLAC.Stanford.EDU et al.

References

[RFC2527] Chokhani and Ford, “Certificate Policy and Certification Practices Framework”, IETF RFC 2527, Mar 1999, http://www.ietf.org/rfc/rfc2527.txt

Change History

3/16/2003 2:01:38 PM

Changes to every section, noted by name, including:

01 Feb 2003 changes from mwh to Introduction

01 Feb 2003 (approx) changes from TG to abstract/introduction to meet editorial requirements

28 Feb 2003 changes from Peter Gietz to Introduction, various sections, and extensive additions to directory, and extensive suggestion for By-Laws, as well as comments on section 8, the examples

10 Mar 2003 (approx) changes from Bob Cowles mostly to section 3, GPMA membership

16 Mar 2003 editorial changes from mwh, to fix headers again, clean up TOC and fix its style, clean up trashed sections and some weird leftover Word debris, merge changes from all the above authors.

September 24, 2003 added changes from list. Reformatted doc.

February 20, 2004 reformatting, section headings, appendix (TG)
Wordsmithing (mwh)