GWD-C
Category: Community Practice GFD

CAOPS Working Group

Mike Helm, ESnet/LBNL
Peter Gietz, DAASI International GmbH
Tony J. Genovese, ESnet/LBNL
October 16, 2002

Policy Management Authority Charter

Status of This Memo

This memo provides information to the Grid community; it is a GGF community practice document. It does not define any standards or technical recommendations. Distribution is unlimited.

Copyright Notice

Copyright © Global Grid Forum (2002). All Rights Reserved.

Abstract

A Policy Management Authority [PMA] for an inter-Grid Certificate Authority [CA] and Public Key Infrastructure [PKI] is described. This is a draft – discussion document and needs to be read in context with the Policy Management Authority slides from GGF-4.

Table of Contents

1. Introduction 2
2. Scope of PMA 2
3. PMA Membership 3
3.1 Creation 3
3.2 New Members 3
3.3 Type of Membership 3
3.4 Membership Guidelines 3
3.5 Executive Council 3
3.6 Withdrawal/Expulsion 3
4. Responsibilities 4
4.1 CP/CPS 4
4.2 Other documents 4
4.3 Audit 4
4.4 Operations 4
4.5 Directory 5
5. Activities 5
Point of Contact 5
5.1 Meetings 5
5.2 Research 5
5.3 Decision – making process 5
6. Bylaws 6
7. Examples 6
7.1 ESnet – DOE Grids PKI 6
7.2 EDG WP-6 CA managers 6
7.3 US Federal Bridge 6
8. Security Considerations 6
9. Author Information 6
10. Glossary 7
11. Intellectual Property Statement 7
12. Full Copyright Notice 7
13. References 7

1. Introduction

This is the PMA charter for the "Global Grid PKI" [GGPKI] and the "Global Grid Certificate Authority" [GGCA]. These may consist of a single CA with one or more points of registration; a bridge between multiple root CA's; lists of acceptable CA's; or other combinations. Since the Grid consists of many different kinds of organizations working towards interoperability, this document will include issues that might not pertain to a single organization. The GGCA may exist or may be a goal during the early period of the PMA. The GGPKI is affiliated with the GGF.

Organizations that deploy a PKI will need a policy management authority. PKI is not an end in itself, but serves various purposes in the Grid community, providing a method for single sign-on, enabling convenient and inexpensive authentication service, and enabling trust between different organizations. The PKI will also support critical authorization services of various types. This trust is entirely dependent on a clear and complete specification of how components of the PKI, or at least the CA, are to be operated. These specifications are found in the Certificate Policy [CP] and Certification Practices Statement [CPS]. These documents are long and complex; the Grid is fast moving, adding new requirements and adjusting old ones. The Grid will consist of many different PKI's and CA's. The PMA will manage the changes resulting from internal pressures. The PMA will serve as point of contact for other PKI's that need to interoperate with the GGPKI, managing external relationships and any resulting internal changes. These changes will be reflected in the CP and CPS documents.

2. Scope of PMA

The PMA'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 CP/CPS should provide contact information for the PMA managing it.

The PMA 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, and the like.

The PMA provides points of contact for external entities – other PKI PMA's, potential new members or relying parties.

In all cases the PMA provides access to

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

3. PMA Membership

3.1 Creation

Members of virtual organizations [VO's] running CA's or in need of CA services agrees to work on an interoperable PKI. These VO's appoint an interim chairman (by consensus). The chairman will ask the GGFSG for formal recognition.

The initial set of members will set up a hosting organization and web site to provide access to the document set and contact information.

The initial set of members will appoint a committee to draft the CP and CPS documents.

The initial set of members will hire an operator of the GGCA.

The initial set of members will add bylaws to the PMA charter to manage the question of new members, and other issues.

3.2 New Members

It is assumed that the GGPKI will add organizations that will operate their own CA's, or their own registration and identity management infrastructures in the GGCA.

New members must agree to abide by the CP/CPS and other documents managed by the PMA.

New members must be willing to join the PMA as participating members.

New members are approved by existing members of the PMA, through a voting process or other means as specified in the bylaws.

3.3 Type of Membership

PMA membership is based on constituent organizations, but is made up of named individuals. An organization can provide multiple members, but should only be entitled to one vote. The PMA should require an introduction "ceremony" for new members.

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 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 PMA.

3.6 Withdrawal/Expulsion

Organizations may cease to exist or drastically change their management. The PMA bylaws should allow for this.

4. Responsibilities

4.1 CP/CPS

These complex documents require on-going revision and examination. The documents as constructed (usually based on RFC 2527) have overlapping sections, and there are usually incompletely developed subsections or mutually contradictory subsections. 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

4.2 Other documents

The PMA manages its own charter, and should add or change by-laws to deal with changing conditions and membership.

- Subscriber (end-entity) and relying party agreements.
- Operations guides – access to these may be controlled due to security considerations.

4.3 Audit

The PMA is responsible for assuring that the GG CA and GG PKI are operated in accordance with the CP/CPS and other operations documents. The PMA will conduct periodic compliance audits of the GGCA , its registration authority operations, and subordinate CA's.

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

The PMA must publish substantial portions of the audit report.

4.4 Operations

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

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

4.5 Directory

X.509 certificate services have hidden or explicit dependencies on directory (LDAP, X.500). The GG PKI's relationship with directory is unclear at this time, but the PMA will include directory management and access with GG CA and GG PKI operations issues.

5. Activities

Point of Contact

The PMA 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 GGPKI this is effectively the world.

5.1 Meetings

The PMA will meet periodically (as described in the by-laws). It may meet on the same schedule as GGF. 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.

5.2 Research

It is expected that Grid requirements and PKI technology will change considerably in the near future. The PMA will support a research committee. This committee may exist in the GGF as a research working group.

5.3 Decision – making process

The PMA needs to provide an orderly decision-making process. The PMA 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 PMA 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 PMA should set aside a review period for all items under consideration, to allow all parties time to understand the issues.

The PMA 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 PMA may choose to establish some other system in its by-laws.

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

6. Bylaws

This section reserved for the PMA to describe its specific requirements.

7. Examples

7.1 ESnet – DOE Grids PKI

http://www.doegrids.org

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

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

7.2 EDG WP-6 CA managers

This is a list of CA's supporting European Data Grid.

http://marianne.in2p3.fr/datagrid/ca/ca-table-ca.html

There is no central CA, and this sub-group doesn't yet characterize itself as a PMA, but it is one in fact. The member CA's operate in similar fashions, the group maintains a kind of specification document, and is managing a compliance audit process.

7.3 US Federal Bridge

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

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

This PKI 's bylaws has influenced the ESnet PKI

8. Security Considerations

The PMA 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.

9. Author Information

Mike Helm
ESnet/LBNL
Helm@ES.net

Peter Gietz
DAASI International GmbH
peter.gietz@daasi.de

Tony J. Genovese
ESnet/LBNL
Tony@ES.net

10. Glossary

None.

11. 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.

12. Full Copyright Notice

Copyright (C) Global Grid Forum (date). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the GGF or other organizations, except as needed for the purpose of developing Grid Recommendations in which case the procedures for copyrights defined in the GGF Document process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the GGF or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE GLOBAL GRID FORUM DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE."

13. References

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