

# The Americas Grid Policy Management Authority Charter

July 18, 2005

# Table of Contents

1.	The Americas Grid Policy Management Authority (TAGPMA) .....	3
1.1	Mission .....	3
1.2	Community .....	3
1.3	Scope of TAGPMA .....	3
1.3.1	Included TAGPMA activities .....	3
1.3.2	Excluded TAGPMA activities .....	4
1.4	Founding members.....	4
1.5	TAGPMA administration services .....	4
2.	TAGPMA Authentication Architecture .....	4
2.1.	Introduction .....	4
2.2.	Supported Authentication service types.....	5
3.	TAGPMA Identity services .....	5
3.1.	Introduction .....	5
3.2.	Operational Authentication services .....	5
3.3.	Experimental or test Authentication Services .....	5
4.	TAGPMA Authentication services Operational requirements .....	5
5.	TAGPMA Site Security .....	5
6.	Publication and Repository Responsibilities .....	6
7.	Liability .....	6
8.	Financial responsibilities .....	6
9.	Audits .....	6
10.	Privacy, confidentiality .....	6
11.	Compromise and Disaster Recovery .....	6
12.	TAGPMA Administration .....	6
12.1.	Introduction .....	6
12.2.	Scope .....	7
12.2.1.	Included TAGPMA activities.....	7
12.2.2.	Excluded TAGPMA activities.....	7
12.3.	Chartering procedure – organizational structure Permanent Society .....	7
12.3.1.	Creation of TAGPMA administration .....	7
12.4.	Membership .....	7
12.4.1.	TAGPMA Chair .....	8
12.4.2.	TAGPMA Secretary.....	8
12.4.3.	TAGPMA Security Officer .....	8
12.4.4.	New or renewing membership process .....	8
12.4.5.	Resignation/Expulsion.....	9
12.5.	Governance .....	9
12.5.1.	Introduction.....	9
12.5.2.	Meetings .....	9
12.5.3.	TAGPMA administration voting .....	9

# **1. The Americas Grid Policy Management Authority (TAGPMA)**

## **1.1 Mission**

The Americas Grid PMA (TAGPMA) is a federation of Grid certification authorities and relying parties operating within the region known as the Americas. It will be governed by a Policy Management Authority (PMA) that consists of members with responsibilities for Grids in the Americas. The goal of the federation is to facilitate the cross domain trust relationships needed to deploy grids in the Americas and globally.

The TAGPMA will be the official body representing this community with other regional PMAs that provide similar services to their Grid communities. Currently there are two other regional Grid PMAs: The EU Grid PMA and the Asian Pacifica PMA. The goal is to establish peering relationships with these other regional PMAs. This peering relationship will be coordinated under the International Grid Trust Federation ([www.gridpma.org](http://www.gridpma.org)). The Chairman of the TAGPMA will be a full voting member on the IGTF PMA.

The community served by the TAGPMA wants help in determining the trustworthiness of authentication service providers in the Americas and the other regional PMAs. It will be the mission of the TAGPMA to develop and maintain published information on the trustworthiness of its member authentication service providers. It will also publish trustworthiness information on authentication service providers that are members of our peer PMAs (i.e. EUGridPMA and APGridPMA). The criteria used to determine trust and the publishing model are the responsibility of the TAGPMA.

The TAGPMA represent a diverse community of authentication service providers. In the other regional PMAs there is only one type of authentication service that is trusted. This service is based on classic PKI and the use of X.509v3 certificates. In the Americas a number of new innovations for providing authentication service are now in service or underdevelopment. Beyond the mission of establishing global trust, the TAGPMA will foster the development and acceptance of new authentication services. The TAGPMA will develop criteria that can be used to evaluate and develop trust in the new services. It will also be the mission to promote these new services with our regional peers.

## **1.2 Community**

The community that will be served by the TAGPMA is the research and academic community in the region know as the Americas. This region stretches from Canada in the North to the tip of Chile in the south and all territories in between.

## **1.3 Scope of TAGPMA**

1. The TAGPMA will provide an accreditation process open to any Grid Authentication service providers in the Americas.
2. The TAGPMA will cover only the territory known as the Americas.
3. The TAGPMA will work on peering with other regional PMAs to develop cross domain trust relationships. This will be coordinated with the International Grid Trust Federation.
4. The TAGPMA will develop criteria for the determining trust in the different types of authentication services.
5. The TAGPMA will accredit member authentication services that meet the TAGPMA criteria for that type of authentication profile.

### **1.3.1 Included TAGPMA activities**

1. The TAGPMA will be responsible for developing Community Best Practices for multiple authentication types/profiles.
2. The TAGPMA will maintain the TAGPMA repository. Items to be included in the repository:

- a. Member contact information
  - b. Root certificates
  - c. Member CP/CPS
  - d. Authentication profile specifications
  - e. Mailing list archives - official votes, etc
  - f. Authentication service provider accreditation
  - g. Letters from members asserting compliance with the TAGPMA policies.
  - h. Other information the TAGPMA considers important to the community.
3. The TAGPMA will hold regular meetings.
  4. The TAGPMA will be responsible for the development and maintenance of minimum requirements for each accredited authentication profile.
  5. The TAGPMA will vote and maintain official records on all issues that represent items that affect a determination of trust in a authentication service.

### **1.3.2 Excluded TAGPMA activities**

1. The TAGPMA will work on accreditation of its members, but will not certify their compliance to our membership rules. It will rely on professional letters of assertion from the accredited member. These letters will be maintained in the TAGPMA repository.
2. The TAGPMA will not run an Authentication or Authorization service for its community.

## **1.4 Founding members**

This list identifies the initial set of participants that will vote on chartering the TAGPMA. The initial membership of the TAGPMA consists of the following:

1. Canarie - Darcy Quesnel
2. OSG - Robert Cowles and Dane Skow
3. TERAGRID - Tony Rimovsky
4. Texas High Energy Grid – Alan Sill
5. DOEGrids - Tony Genovese and Mike Helm
6. SDSC - Bill Link
7. FNAL - Frank Nagy
8. Dartmouth – Mark Franklin and Scott Rea
9. Umich - William Adamson, Olga and Kevin
10. Brazil - Jerome van de Graaf

## **1.5 TAGPMA administration services**

The TAGPMA will maintain systems that support its mission. These systems are not critical to the operation of our members or their relying parties. They consist of our:

- Publishing website
- Repository for our communications and documents
- Root CA repository

## **2. TAGPMA Authentication Architecture**

### **2.1. Introduction**

The TAGPMA Authentication Architecture is a publishing model that consists of our member's authentication services. The TAGPMA will provide trusted access to critical information that can be used by relying parties to build trust relationships from our members Authentication services.

TAGPMA works to coordinate information for use by its members, peering with other regional PMAs and relying parties. TAGPMA does not operate an Authentication system or systems. Authentication services are provided by our members to their communities. Operational requirements for these systems are published and maintained by the TAGPMA.

The TAGPMA will develop Authentication Service profiles that reflect our community's requirements. Each profile will specify the architecture and operational requirements. These profiles will be used to certify a member's authentication service. It will also be used by relying parties to evaluate the authentication service to establish trust in the service.

## **2.2. Supported Authentication service types**

The TAGPMA community's Authentication systems are primarily PKI based systems for use in a Globus enabled grid. The TAGPMA will review various Authentication systems used by our members and publish a list of trusted Authentication profiles. (e.g. Classic PKI, KCA, credential repositories, etc.)

The TAGPMA is not limited to PKI only systems. Based on our community needs, the TAGPMA will review Authentication service providers that wish to establish trust relationships with our relying parties.

## **3. TAGPMA Identity services**

### **3.1. Introduction**

The TAGPMA does not itself run an Identity service. Its members may run these types of services. TAGPMA will establish and maintain operational requirements for its members. By publishing minimum requirements for membership operation of Identity services, we can represent the identity provider in the global peering process.

Our community will consist of production and experimental level Authentication services. Experimental class of services is allowed in our community to experiment and innovate with Authentication services. These services will be marked as experimental and relying parties should act accordingly.

All Production Authentication services will be documented by the TAGPMA and communicated to our peer PMA's with the level of trust we believe should be associated with the service.

### **3.2. Operational Authentication services**

The TAGPMA will maintain a list and archive of its member production Authentication services. This list will be a trusted publishing point for relying parties and our peer PMAs.

### **3.3. Experimental or test Authentication Services**

The TAGPMA will maintain a list and archive of its member experimental Authentication services. This list will be a trusted publishing point for relying parties and our peer PMAs.

## **4. TAGPMA Authentication services Operational requirements**

The TAGPMA will maintain a list of Authentication service operational requirements for each type of service that the TAGPMA has registered. Some of these Operational requirements will be developed by the TAGPMA and maintained on our site. Our Peer PMAs have developed operational requirements for certain types of Authentication services. The TAGPMA will review these requirements for appropriateness for our community. If it is deemed appropriate for our community the TAGPMA will vet the requirements for its community. In this case the TAGPMA will not work on the requirement directly, but will depend on our peer PMA to do this development.

If an external PMA is responsible for developing an Authentication operational requirements document, they will be the primary author and publishing point. The TAGPMA will maintain a copy or link to the authoritative source for the document.

## **5. TAGPMA Site Security**

The TAGPMA will maintain a trusted publishing point for our community. This system must be protected and available to our community. The systems that support this service and the security controls that have been installed must be documented and reviewed by the TAGPMA.

## **6. Publication and Repository Responsibilities**

The TAGPMA will maintain a trusted website for our community. This website will contain information that is open to the general community and information that is restricted to members only. Some of the information that will be maintained on the site:

- Authentication profiles
- Mailing list archives
- Membership directory
- Member CA certificates
- Member CA CRLs.
- Member CP/CPS
- Other supporting documentation.

The operation of this website will be done by Canarie and can be found at:

[www.TAGPMA.org](http://www.TAGPMA.org)

## **7. Liability**

The TAGPMA does not accept any liability to the content of our website or the operational integrity of our members. It is the responsibility of the relying party to verify all information that it uses.

## **8. Financial responsibilities**

The TAGPMA is operated as a cooperative endeavor. All financial costs are absorbed by our members. The TAGPMA is not financially responsible for any of its members.

## **9. Audits**

No audits are planned with respect to our member's compliance with our operational requirements.

## **10. Privacy, confidentiality**

No personal information will be maintained about our community. Members will provide contact and email information as needed to participate on mailing lists or identification of participation in the TAGPMA.

## **11. Compromise and Disaster Recovery**

The TAGPMA systems used to provide our community with information must have a disaster recovery plan. This plan will be maintained and audited by the TAGPMA. The plan must address how the service will function and provide community access during and after a disaster.

## **12. TAGPMA Administration**

### **12.1. Introduction**

This section of the TAGPMA charter describes the management process used by the TAGPMA. The following sections describe the scope and limits of the TAGPMA. It describes how members can join or leave the organization. Also, how the decisions are to be made by the TAGPMA.

## **12.2. Scope**

The TAGPMA will hold regular meeting at which time they can discuss and possibly vote on the following types of items:

1. The accreditation process for Grid Certificate Authority in the Americas.
2. The territory covered by this PMA.
3. Peering with other regional PMAs to develop cross domain trust relationships.
4. Coordination of our peering with the International Grid Trust Federation.
5. The multiple Grid Authentication methods used by our community.

### **12.2.1. Included TAGPMA activities**

1. The TAGPMA will be responsible for developing Community Best Practices for multiple authentication profiles.
2. The TAGPMA will maintain the TAGPMA repository. Items to be included in the repository:
  - o Member contact information
  - o Root certificates
  - o Member CP/CPS
  - o Mailing list archives - official votes, etc
3. The TAGPMA will be responsible for the development and maintenance of minimum requirements for each accredited authentication profile.
4. The TAGPMA will review members that run authentication services based on an approved Authentication profile and certify the operator is professionally committed to running the service to our specifications. This will not include a physical compliance audit.

### **12.2.2. Excluded TAGPMA activities**

1. The TAGPMA will work on certification of its members, but will not physically audit their compliance to our operational rules.
2. The TAGPMA will not run an Authentication or Authorization service for its community.

## **12.3. Chartering procedure – organizational structure Permanent Society**

The initial TAGPMA will consist of the founding members. The transition from a chartering organization to TAGPMA will occur after the founders vote on the charter. This charter will become the administrative controlling document of the TAGPMA.

The TAGPMA will be organized as a permanent society. It will be established by a majority vote of the founding members. The vote will occur when the founding members believe this charter is sufficient to describe and manage the TAGPMA. After chartering the TAGPMA will be administered by the by-laws outlined in this subsection.

### **12.3.1. Creation of TAGPMA administration**

The first official meeting of the TAGPMA will occur directly after the charter is approved by the founders. The first task of the new TAGPMA will be to elect the 3 officers of the TAGPMA. Each year on the anniversary of the original election new elections will be called by the Chair. After the calling of the election the general TAGPMA body can nominate individuals to fill the open roles.

## **12.4. Membership**

There are two types of members on the TAGPMA.

- TAGPMA officers
  - Chairman
  - Secretary
  - Security Officer
- General voting members

The TAGPMA General voting members will consist of individuals drawn from our user community in the Americas. As grids are being deployed today they are crossing physical or logical site boundaries. 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 (VOs)
2. Large research sites in the Americas
3. Universities

The TAGPMA will consist of people having the following community roles:

1. Certificate Authorities. Responsible for approval or revocation of certificates issued to their community.
2. Relying parties representing communities that depend on the trust worthiness of certificates.
3. Authentication service providers other than PKI based.

#### **12.4.1. TAGPMA Chair**

The TAGPMA community will elect a chair to manage the TAGPMA. Only members of the TAGPMA can run and be elected as Chair. The term as chair is to be one year. The chair may resign by written request to the TAGPMA. The TAGPMA, by vote can remove the Chair. The chair is responsible for:

1. Point of contact for the TAGPMA
2. Liaison to EUGridPMA and the Asian Pacific PMA
3. Member of the International Grid Trust Federation PMA.
4. Running the TAGPMA meetings
5. Insuring Minutes are taken and published.
6. Insuring that all voting is recorded and published

#### **12.4.2. TAGPMA Secretary**

Only members of the TAGPMA can run and be elected as secretary. The TAGPMA 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 repository.
3. Email list membership.
4. Coordinate editing and publishing of all PMA documents.
5. Handle all letters community service as submitted by new or renewing members.
6. Must certify the vote and record in the archive the official outcome of each vote the TAGPMA holds.

#### **12.4.3. TAGPMA Security Officer**

Only members of the TAGPMA can run and be elected as Security Officer. The TAGPMA 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 TAGPMA.
2. Oversight of the any Security incident handling committee required.
3. Liaison to other PMAs staff to handle security reporting and response.

#### **12.4.4. New or renewing membership process**

The TAGPMA will add new members over time. New Virtual Organizations (VO), Sites and Universities will be added to the TAGPMA. Each new site, VO or University 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 TAGPMA.

The term of membership for all TAGPMA members will be for one year.

To become a member the candidate needs to submit a letter to the TAGPMA describing the community in the Americas to be served. Annual renewal of their membership will occur by submitting or resubmitting their letter of community service.

The TAGPMA Secretary will maintain the letters of community service and acknowledge the continued membership or removal of non performing members.

#### **12.4.5. Resignation/Expulsion**

All members of the TAGPMA can resign by submitting a letter to the Secretary of the TAGPMA. Members can be removed from the TAGPMA for:

1. Non compliance to operational requirements established by the TAGPMA
2. Non renewal of community commitment.

### **12.5. Governance**

#### **12.5.1. Introduction**

This section describes the process by which the TAGPMA will meet and the decision process used by the PMA.

#### **12.5.2. Meetings**

The TAGPMA will meet quarterly or as required, to conduct routine business at a time and place announced by the Chair. An agenda is prepared in advance and electronically 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:

1. Membership changes within the current TAGPMA
2. Applications for membership to TAGPMA.
3. Changes to policies or other Authentication management directives
4. Review of Authentication-related procedures and record-keeping practices of its members
5. Incidents and non-routine events
6. Interfaces with other organizations
7. Changes in standards or technology

Minutes of each meeting must be taken and archived. The minutes must be approved by the TAGPMA for publication and entry to the archive.

#### **12.5.3. TAGPMA administration voting**

The TAGPMA approval is arrived at by either obvious consensus as determined by the chair or by a vote. When the TAGPMA must vote to fulfill its obligations, that vote will be made by a quorum of the TAGPMA members. A quorum is defined as more than 50% of the current PMA membership. A positive vote will be recorded if more than 50% of the voting quorum votes in favor of the proposal. The vote can be carried out at an official meeting of the TAGPMA or over a specified period of time. If the vote is to be covered by a voting period the voting period will be a minimum of 10 working days. All votes must be conveyed to the TAGPMA chair by using digitally signed email. If the vote occurs during a scheduled meeting the proposal and its associated voice vote will be recorded in the minutes of the meeting. If the vote is carried out over a time period, at the close of the time period the Chair must post the proposal and official count of votes to the TAGPMA archived mailing list. The minutes or the Chair's voting summation will be the official record of the voting process. Each official vote will include the proposal and the members name and their vote as: For the proposal, against the proposal or Abstention.