

The Americas Grid Policy Management Authority Charter

Nov. 9, 2007

Version 2.2

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
1.4	General TAGPMA activities	4
1.5	Founding members	4
1.6	TAGPMA administration services	4
2.	TAGPMA Authentication Architecture	4
2.1.	Introduction	4
2.2.	Supported Authentication service types	4
3.	TAGPMA Identity services	5
4.	TAGPMA Authentication services Operational requirements	5
5.	TAGPMA Site Security	5
6.	Publication and Repository Responsibilities	5
7.	Liability	5
8.	Financial responsibilities	5
9.	Audits	5
10.	Privacy, confidentiality	5
11.	Compromise and Disaster Recovery	6
12.	TAGPMA Administration	6
12.1.	Introduction	6
12.1.1.	Administrative Scope and Activities	6
12.1.2.	Excluded TAGPMA activities	6
12.2.	Chartering procedure – organizational structure Permanent Society	6
12.2.1.	Creation of TAGPMA administration	6
12.3.	Membership	6
12.3.1.	TAGPMA Chair	7
12.3.2.	TAGPMA Secretary	7
12.3.3.	TAGPMA Security Officer	7
12.3.4.	New or renewing membership process	7
12.3.5.	Resignation/Expulsion	8
12.4.	TAGPMA Governance process	8
12.4.1.	Introduction	8
12.4.2.	Meetings	8
12.4.3.	TAGPMA administration voting	8
13.	General Definitions	9
14.	Change log	10

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). 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. The goal of selecting a region is to facilitate the development and deployment of Authentication services for our community. Areas covered by regional PMAs may at times overlap, the selection of a PMA is up to the service provider. The local regional PMA should be preferred over a remote PMA to insure timeliness and convenience.

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 peer 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 or new types of authentication services.
5. The TAGPMA will accredit member authentication services that meet the criteria for a particular authentication profile that covers the specific authentication service under review.
6. The TAGPMA will accept and encourage input on Authentication Services from other regional PMAs.

1.4 General TAGPMA activities

1. The TAGPMA will hold regular meetings.
2. The TAGPMA will be responsible for developing Community Best Practices for multiple authentication profiles.
3. The TAGPMA will be responsible for the development and maintenance of minimum requirements for each accredited authentication profile.
4. The TAGPMA will vote and maintain official records on all issues that represent items that affect a determination of trust in an authentication service.
5. The TAGPMA will accredit of it's AS providers and document their compliance to approved ASs.
6. The TAGPMA will help investigate security issues raised by members or from members of the IGTF.

1.5 Founding members

The TAGPMA was chartered in September 2005 by the following organizations in the Americas:

1. Canarie
2. Open Science Grid
3. TeraGrid
4. Texas High Energy Grid
5. DOEGrids
6. SDSC
7. FNAL
8. Dartmouth

1.6 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
- Trust anchor repository
- Other services and information as defined by the TAGPMA.

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 or adopt Authentication Service profiles that reflect our community's requirements. Each profile will specify the architecture and operational requirements. These profiles will be used to accredit 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 by our member communities. The TAGPMA will review various Authentication services used by our members and publish a list of trusted Authentication profiles.

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.

The TAGPMA will specify and maintain a list of Authentication Profiles to be used for accreditation that are agreed upon in collaboration with other IGTF member PMAs.

3. TAGPMA Identity services

The TAGPMA does not itself run an Identity service.

4. TAGPMA Authentication services Operational requirements

The TAGPMA does not itself run an Authentication service.

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:

- Member contact information
- Trust Anchors
- Member Policy and Practices documents required by AS (eg cp/cps)
- Authentication profile specifications
- Mailing list archives - official votes, etc
- Authentication service provider accreditation
- Letters from members asserting compliance with the TAGPMA policies.
- Other information the TAGPMA considers important to the community.

The operation of this website will be carried out by a specific TAGPMA member upon approval by the group and can be found at: <http://www.TAGPMA.org>. This responsibility can be transferred to another TAGPMA member upon mutual agreement after notification to the rest of TAGPMA.

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 to meet the goals and scope outlined above. It describes how members can join or leave the organization. Also, how the decisions are to be made and recorded by the TAGPMA.

12.1.1. Administrative Scope and Activities

The TAGPMA will hold regular meeting at which time they will work on items that fall under their scope and activities as defined in section 1 above. These activities may require the development and publishing the group's consensus. The development of group consensus may require voting by its members. The minutes and votes will be recorded in the TAGPMA repository. The TAGPMA meetings may be face to face meetings or supported by other technical means.

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 may include a physical compliance audit.

12.1.2. Excluded TAGPMA activities

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

12.2. Chartering procedure – organizational structure Permanent Society

The initial TAGPMA consisted of the founding members. The transition from a chartering organization to TAGPMA occurred after the founders voted on the charter as described below. This charter is the administrative controlling document of the TAGPMA.

The TAGPMA is organized as a permanent society. It was established by a majority vote of the founding members.

The TAGPMA founding members voted in Sep 2005 to establish the TAGPMA.

12.2.1. 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.

12.3. Officers and Membership

There are two types of members on the TAGPMA.

- TAGPMA officers
 - Chairman
 - Vice Chair
 - Secretary
 - Other officers as defined below
- General voting members

1. The TAGPMA General voting members will consist of a representative from each accredited Authentication Service provider in the Americas. Voting members may also be drawn from any of the major Relying Parties of the accredited Authentication Service provider.

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.

The list of officers and members for the TAGPMA is officially recorded on the PMA website.
<http://www.tagpma.org/>

12.3.1. 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 Asia Pacific Grid PMA
3. Voting member of the International Grid Trust Federation PMA.
4. Running the TAGPMA meetings
5. Ensuring Minutes are taken and published.
6. Ensuring that all voting is recorded and published
7. Ensuring that CAs receiving accreditation are included in the IGTF distribution

12.3.2. TAGPMA Vice Chair

8. The TAGPMA community will elect a vice chair to assist the Chair upon request in the conduct of the above duties. Only members of the TAGPMA can run and be elected as Chair. The term as chair is to be one year. The Vice Chair may resign by written request to the TAGPMA. The TAGPMA, by vote can remove the Vice Chair.

12.3.3. 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 document repository and web site.
3. Email list membership.
4. Coordinate editing and publishing of all PMA documents.
5. Handle record-keeping with respect to TAGPMA membership.
6. Must certify the vote and record in the archive the official outcome of each vote the TAGPMA holds.

12.3.4. Other TAGPMA Officers

1. The Chair can appoint other TAGPMA members to fill operational positions for the internal operations of the organization. Notification of such appointments should be made to the general TAGPMA membership as soon as possible and discussed at the next TAGPMA meeting.

12.3.5. 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 two years.

NEEDS WORK:

To insure consistency and quality of our membership, the TAGPMA has chosen to use the same process for membership accreditation that is used by the EUGridPMA. The EUGridPMA maintains the Accreditation Procedures document in its repository:

<http://www.eugridpma.org/guidelines/>

12.3.6. 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.

ADD TO THIS SECTION TO ADDRESS PROCEDURES

12.4. TAGPMA Governance process

12.4.1. Introduction

This section describes the processes used by the TAGPMA to meet the responsibilities of its scope and administration activity. To accomplish these goals the TAGPMA uses regular meetings and a consensus building or voting process.

12.4.2. 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.

12.4.3. 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.

13. General Definitions

Authentication Profile (AP)

An Authentication Profile consists of an Authentication service and a community definition on how the service is to be defined and operated. The use of the GGF Authentication Federation Profile document will help facilitate cross trust between Authentication service providers. The goal of the Authentication Profile is to allow relying parties the ability to technically review the service. Also it helps them to judge the trust worthiness of the service.

Authentication Service (AS)

A service that provides trusted identification tokens to a community. This service could use a number of technologies to provide identity tokens. Possible choices: X.509, Kerberos, One Time passwords, Active Credential Stores, Site integrated Proxy services.

Certification Authority (CA)

The entity / system that issues X.509 identity certificates (places a subject name and public key in a document and then digitally signs that document using the private key of the CA

Certificate Policy (CP)

A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.

Certification Practice Statement (CPS)

A statement of the practices, which a certification authority employs in issuing certificates.

Host Certificate

A Certificate for server certification and encryption of communications (SSL/TSL). It will represent a single machine. Host Certificates are used internally by the PKI service and are not issued to other sites/VOs

Person Certificate

A certificate used for authentication to establish a Grid Person Identity. It will represent an individual person.

Policy Management Authority (PMA)

This is a committee composed of the CA managers and representatives from the site/VO Registration Authorities. A PMA usually has responsibility for the CP/CPS and oversight of operations of a PKI. Other APs maybe approved and managed by a PMA.

Point of Contact

A person from a site, VO or University serves on the TAGPMA and represents their organization. This person will handle all communications about policy matters with the TAGPMA and the organization they represent.

Policy Qualifier

The Policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate.

Registration Authority (RA)

An entity that is responsible for identification and authentication of

certificate subjects, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).

Registration Agent (RAg) or “Agent”

RAg is the entity that interacts with the PKI in order to cause the CA to issue certificates.

Relying Party

A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.

Security Incident

An incident that has the potential of private key loss or compromise, regardless of if the compromise or loss was successful. Such incidents include but are not limited to user credential compromise, privilege escalation on systems known to contain private keys, accidental exposure of private keys to unauthorized third parties or loss of a private key.

Service Certificate

A certificate for a particular service running on a host. It will represent a single service on a single host.

Subscriber

Or sometimes called End Entity is the person who applied for and was issued a certificate.

Virtual Organization (VO)

An organization that has been created to represent a particular research or development effort independent of the physical sites that the Scientist or Engineers work at.

14. Change log

VERSION	DATE	CHANGES
1.0	July 18, 2005	Initial Release based on GGF Authentication Federation Document.
1.1	September 20, 2005	<ol style="list-style-type: none"> 1. Modified community definition 2. Mod Scope and Activities 3. Mod repository responsibilities 4. Mod Administrative Scope and Activities 5. Mod TAGPMA governance intro. 6. Added Glossary
2.0	April 20, 2006	<ol style="list-style-type: none"> 1. Change date and version 2. Remove many highlighted text. 3. Modified founding members to list only organization names. 4. in 2.2 removed reference to APs. Corrected SLCS name. 5. 12.1.1 and 12.1.2 changed will not to may do compliance audits. 6. 12.2 added the founding date for the TAGPMA. 7. 12.3 changed membership rules. 8. 12.3 added pointer to TAGPMA members on website. 9. 12.3.1 and 12.3.2 modified Chair

		<p>and Secretary descriptions. The chair is a voting member of IGTF and the secretary handles formal communications.</p> <p>10. 12.3.4 changed it to state the TAGPMA used the EUGridPMA accreditation procedures.</p>
2.1	Oct. 23, 2007	<ol style="list-style-type: none"> 1. Updated officers and position descriptions 2. Correct to past tense where appropriate. 3. Add item on transfer of web site responsibilities.
2.2	Nov. 9, 2007	<ol style="list-style-type: none"> 1. Revised Chair and Secretary responsibilities 2. Updated procedures for ancillary positions.