Category: guidelines document
Status: DRAFT
Document: EUGridPMA-accreditation-20120116-2-1.doc
Editor: davidg
Last updated: Fri, 13 January 2012

Accreditation and Membership Process Guidelines

Abstract
This Guideline describes the processes by which members are accepted into the EUGridPMA. Ist described the accreditation process for Authority members, and the requirements placed on members with regards to auditing and continued participation in the PMA.

Table of Contents

1 Membership Requests

Any community or organisation eligible for membership under the Charter of the EUGridPMA can apply for such membership by sending a request to the PMA Chair[1]. Requests for membership may be submitted on paper or in electronic form, should contain enough information to verify eligibility of the prospective member.

The following information should be presented in the membership request:

- Name of the organisation applying for membership
- Contact information for the applying organisation, including both physical and electronic addresses
- Name and contact information of one primary and at least one alternate representative of the organisation
- Description of the constituency to be represented. For prospective Authority members, this information should include the geographical extent of the authority and the constituency served within that geographical extent, and the Authentication Profile(s) under which the authority aims to be accredited. For prospective Relying Party members, this information should include the constituency represented, as well as a rationale as to why this constituency is not already represented through the existing Authority members single or combined.
- Prospective Authority members should describe how their organisation has or will ensure appropriate and comprehensive coverage of the indicated geographical area and the target constituency therein.

1.1 Constituency and coverage

The goal is to serve the largest possible e-Science community with a small number of stable CAs. Considerations that limit the number of accredited authorities include those of manageability, the ability to ensure a high and consistent level of security of all accredited authorities through auditing and review, and technical considerations – including those related to the total number of distributable trust anchors to relying parties.

To achieve sustainability each CA should be operated as a long-term commitment by institutions or organizations, and be supported by a well-established legal entity, rather than being bound to specific projects or events. The goal is to serve the largest possible community with a small number of stable CAs. The CA structures being accredited, and the constituencies served, should be aligned with the Charter and with the scope of the EUGridPMA as an international coordination body.

1.2 Moderation

The PMA, or its Chair acting on behalf of the PMA, may moderate any incoming requests to ensure the procedural guidelines and the requirements and intent of the Charter are met and that the PMA can meets its objectives in ensuring an operational authentication infrastructure for e-Science. The Chair may consult confidentially with current PMA members on this matter if so required.

1.3 In-person appearance

Membership can be granted and authorities accredited only in a face-to-face PMA meeting, and then only after an in-person appearance of a representative of the membership applicant.
The PMA may grant provisional membership without an in-person appearance only on proposition by the Chair, and then only by consensus of the current PMA membership. In such cases an additional vote must be conducted by e-mail. Provisional membership is valid no longer than till the next meeting.

[1] The Chair, with agreement of the PMA, may delegate tasks described in this Guidelines. This Guideline then applies to the Chair and to any person who hold such a delegated responsibility.

1.4 Gaining membership

In accordance with the Charter, prospective Authority members will only gain membership status after at least one of their issuing authorities has been distributed by the PMA or the IGTF. Prospective Relying Party members gain membership status following approval by the PMA.

By becoming member of the PMA, the organisation and its representatives understand and agree to participate in the activities of the PMA and contribute in-kind to its organisation and operations, and to the PMA processes that support the trust in the authentication infrastructure. This includes but is not limited to periodic face-to-face participation in its meetings at least annually, and meeting any on-going requirements expressed in the relevant Authentication Profiles, the PMA Charter and the IGTF Federation Document.

2 Accreditation process for Authorities

The PMA will accredit Authorities based on the positive outcome of an initial review with respect to all relevant guideline documents, and a successful registration process.

1. The applicant send a request for accreditation to the Chair. Once accepted by the chair in accordance with section 1 and subject to moderation, the application and acceptance and the accreditation process starts. This event is registered in the internal PMA repository and contact data posted there.

2. The Chair will ensure that the applicant representatives are subscribed to the relevant communications media, including the PMA discussion email list, so as to be able to participate in discussions regarding their application.

3. The Chair will announce the prospective member to the PMA discussion list, and provide the PMA with the organisational information, the names of the representatives, the description of the constituency, and the intended Authentication Profile.

4. The Chair will solicit at least two reviewers from amongst the current PMA membership, who will guide the review of policy and practices documents as well as operational issues.

    a. If the applicant already has an existing set of policies and practices, the reviewers may commence their review forthwith
    b. If the applicant has not yet completed a set of policies and practices, it is recommended that the applicant works with the assigned reviewers and other PMA members when drafting these documents.

    Major versions of the documents sent to the reviewers will be made available to the Chair for posting on the internal review web site and scrutiny by all PMA members.
    If specific practices of the CA are considered confidential by the applicant, the PMA by consensus may exceptionally agree to keep such information distribution limited to the assigned reviewers only. Such practices should then be described in separate documents.

5. The review process is iterative, and is expected to continue until consensus between the reviewers and applicant is reached. The Chair is kept informed of major changes and milestones in the review process, for recording on the internal web site. Reviews and the iterations are expected to occur at regular intervals, at least monthly.

    In case of non-convergence, the Chair may appoint additional reviewers, and/or moderate the process. In all cases, the final decision rest with the PMA as a whole, according to the rules laid down in the Charter.

6. The applicant should make a face-to-face presentation discussing each authority at a plenary meeting of the PMA. This may happen at any time during the accreditation

process, but the presentation should contain substantive information about the authority and should substantially present the final situation.
The presentation must discuss all important elements of the authority, including the authentication model, identity vetting model, and naming, as well as physical security measures, record keeping, and auditing.
The presentation and documentation should substantially match the results of the self-audit based on the guidelines for the specific Authentication Profile.

7. Once the presentation is held and both the reviewers and the Chair, or the PMA in session, deems that the presented policies, practices and their implementation meet the requirements, the Authority may be approved.

8. Approval of an Authority is based either on clear consensus or by voting.

    a. The PMA in session can decide to grant provisional approval in case only minor issues remain before the Authority can be fully approved. The intended consensus can then be reached after the definitive version of the documents is made available and known to the PMA and no objections have been raised on the email list in the following 10 working days.

After definitive approval and distribution of at least one issuing authority, the prospective Authority will become a member, gain all associated rights and duties, and will be included in the membership list.

3 Registration process

Before an accredited authority can be included in the repositories of the PMA the relevant introduction ceremonies must be completed successfully.

The following information must be conveyed to the PMA Chair – by a trusted means if required due to the nature of the information. This includes all information described in the relevant guideline documents and Authentication Profile under which an authority is accredited, and must additionally include:

- Name of the organisation responsible for the accredited authority(ies)
- Contact information for the organisation, including both physical and electronic addresses
- Name and contact information of one primary and at least one alternate representative of the organisation
- An email address used for communicating concerns and requests to the Authority
- URLs where the policy and practices document(s) are made available to interested parties;
- URL to a web page containing general (subscriber-oriented) information of the authority
- URLs to all trust anchors and to relevant revocation information
- Fingerprint(s) of the trust anchors or root certificate(s);

The introduction process is not complete until all the information above has been conveyed to the PMA.

3.1 Namespace assignment

The PMA, in coordination with the authority, will assign a unique non-overlapping name space to each member for subject distinguished names for those subjects that are to be considered part of the PMA and IGTF trust infrastructure.

The member is encouraged to ensure that the namespace information, including its technical implementations, proposed for inclusion in the PMA and IGTF distribution is correct and complete, and reflects the agreement between the member and the PMA.

4 Distribution of Trust Anchors

Following approval and having completed the introduction ceremonies and the registration of trust anchors and meta-data successfully, the trust anchors pertaining to the Authority will be included in the Common Source repository of the International Grid Trust Federation (IGTF) and the PMA. These trust anchors and associated meta-data will be included in the relevant trust anchors distributions issued thereafter. Distribution of trust anchors will be in accordance with the Authentication Profile under which an issuing authority has been accredited.

Distribution of trust anchors may be postponed or suspended if inclusion in the distribution leads to operational problems in the authentication infrastructure. The PMA Chair and/or the Risk Assessment Team of the PMA and the IGTF will assess any operational issues related to the distribution of trust anchors. Trust anchors should comply with relevant standards.

The PMA and the IGTF periodically issue publicly a versioned distribution containing trust anchors and their associated meta-data. The frequency of publication is decided by the PMA and IGTF, having considered requirements on accuracy, timeliness, scalability and implementation of the trust anchors by relying parties, and having heard requests for publication by its membership.
The format of the distribution is decided by the PMA and the IGTF, having considered requests from its members and the general public, and bearing in mind the implementation of the authentication infrastructure and availability of resources within the PMA and IGTF.

The Chair is kept informed of major changes and milestones in the review process, for recording on the internal web site. In case of non-convergence, the Chair may appoint additional reviewers, and/or moderate the process. In all cases, the final decision rest with the PMA as a whole, according to the rules laid down in the Charter.

5 Modifications

Material changes in the policies, practices and issuing name space may void the accreditation unless approved beforehand by the PMA.

A planned change in policy, practices or namespace where the new policy is expected to qualify under the same Authentication Profile under which the issuing authority is currently accredited, must be submitted to the PMA for approval and such a request must contain at least the following information:

- Name of the Authority
- List of trust anchor(s) involved with the change
- A summary of relevant changes
- Other information to facilitate a comparison between the current and proposed policy by any qualified PMA member within a reasonable amount of time. Specifically, such other information may include a marked-up list of changes in the new document, detailing those elements that have changed since the previous version
- The date on which the new policy is proposed to go into effect

Any PMA member should be given the full opportunity to read and react to changes. To this effect, both the new document and the old document(s) must be made available to PMA members, and an announcement on where these document may retrieved must be circulated on the PMA member mailing list.
On request of the Authority or on its own initiative, the PMA Chair can facility the availability by making such document(s) available in the (internal) PMA repository.

Complaints should be raised within two work-weeks after announcing the changes. If any such complaints are raised, the proposed modification is held until the issues are satisfactorily resolved.

Resolution may be by vote or by tacit consent as determined and announced by the Chair. If no objections are raised, the proposed changes are approved by tacit consent following a two work-week period, as determined and announced by the Chair.

Changes in policy that would result in the CA violating the Authentication Profile under which it is currently accredited cannot be approved. In such cases, a full accreditation based on the new Profile must ensue.

6 Self-audit

Accredited Authorities must perform self-audits in accordance with the Profile under which they are accredited. These results should be presented to the PMA periodically, with an intended frequency of every two years, for peer review by the PMA.

The self-audit results presented should include all important elements of the authority, including the authentication model, identity vetting model, and naming, as well as physical security measures, record keeping, and auditing. In addition, the self-audit should be assessed based on the information and guidance laid down in GFD-I.169 and follow the structure proposed therein, in accordance with the Authentication Profile under which the Authority is accredited.

The Chair will solicit at least two members to peer-review the self-audit results presented, who will review the results and, if so required in order to meet the latest Authentication Profile requirements, monitor progress of the implementation of any changes needed.

7 Communications channels

The PMA maintains the following communications channels pertaining to the accreditation and membership processes

- A public web site listing all current members and their contact addresses.
  This shall be hosted at https://www.eugridpma.org/

- An internal web site listing current applicants, their accreditation process status, and relevant documents and reviews, and other confidential information.
  This shall be hosted at http://www.eugridpma.org/review/

- A discussion mailing list to which all members and selected third parties are subscribed. This list is to be used for general discussions that have no immediate security implications and do not disclose vulnerabilities or would otherwise damage the trust infrastructure.
  This shall be contact via dg-eur-ca@services.cnrs.fr

- A set of contact email addresses for the PMA in relation to accreditation, in particular
  - chair@eugridpma.org for contacting the current Chair
  - info@eugridpma.org for questions regarding the accreditation process
  - concerns@eugridpma.org for any concerns by third parties, including concerns regarding the accreditation process

In case of problems with the Internet domain name system or specific TLD operators, information will be posted on alternative domains, specifically www.eugridpma.info and www.gridpma.eu.