Category: charter documents
Status: DRAFT
DocId: IGF-Federation-20050510-0-2.doc
Editor: David Groep
Last updated: Tue, 10 May 2005
Total number of pages: 6

IGTF Draft Federation Document

Abstract

This document attempts to follow the Federation Document template as defined in the Authentication Profiles Information document of the GGF CAOPS WG.

Table of Contents

1 Federation Definition

1.1 Description of the Federation

The International Grid Federation (IGF) is a body to establish common policies and guidelines for Regional and Continental Policy Management Authorities (PMAs) and to ensure compliance to this Federation Document amongst the participating PMAs. The IGF does not provide identity assertions but instead asserts that – within the scope of this federation document – the assertions issued by accredited authorities of any of its member PMAs meet or exceed an authentication profile relevant to the accredited authority.
This document is authoritative for all operations and actions of the IGF.

1.2 Membership

The International Grid Federation consists of the Asia Pacific Grid Policy Management Authority, the European Grid Authentication Policy Management Authority in e-Science, and The Americas Grid Policy Management Authority.

2 General Architecture

The member PMAs are responsible for accrediting authorities that issue identity assertions. They do not them selves issue such assertions; the authentication authorities provide identity assertions for use in inter-organisational resource access.
The federation maintains a set of authentication profiles (APs) that specify the policy and technical requirements for a class of identity assertions and assertion providers. Each authority is subject to the policies and practices of a specific AP.

The federation maintains one authentication profile:

- Traditional X.509 Public Key Certification Authorities with secured infrastructure

For each AP different stipulations regarding identity management, operational requirements, and site security may be in effect.

2.1 Traditional X.509 Public Key Certification Authorities with secured infrastructure

Traditional X.509 Public Key Certification Authorities (traditional PKI CAs) issue long-term credentials to end-entities[1], who will themselves posses and control their key pair and their activation data. These PKI CAs act as a independent trusted third party for both subscribers and relying parties within an infrastructure.
These authorities will use a long-term signing key, which is stored in a secure manner as defined in the AP.

3 Identity

The federation will ensure that every identifier issued by an accredited authority, under any authentication profile, by any PMA, is associated with one and only one identity, within the scope of the federation.
In case the identity refers to a natural person, this identity shall be forever bound to this one entity, to the extent that this can be realistically validated.
In case the identity refers to a network entity, the network entity must have an assigned natural person named as a responsible for this entity. This responsible person may assign or transfer responsibility for the network entity to another natural person. Every accredited authority must specify a mechanism for dealing with network entities whose responsible person fails in their responsibilities for a network entity without assigning a new responsible for this network entity.

[1] long-term is defined as lasting more than 10 million seconds, i.e., more than approx. two weeks.

Each authentication profile must specify guidelines defining how the binding between identifiers, identities, and entities is managed and maintained.

3.1 Management and communication of identifiers

On accreditation, a specific subject name space or set of subject name spaces is allocated to each authority. This namespace must not overlap with any existing name space already assigned to an existing authority for any AP, assigned by any of the regional PMAs within the International Grid Federation.
The assignment of a namespace to an authority will be according to current best practices, and the name space shall have a reasonable relationship to the scope of the authority. Any proposal for namespace assignment shall be circulated amongst all PMAs within the International Grid Federation, and the assignment will not be permanent unless positive confirmation of uniqueness has been received from all PMA chairs.
Each PMA will distribute widely the list of assigned subject name spaces.

3.2 Identity vetting rules

Each accredited authority must document its identity vetting rules and this document must be publicly available. Changes to this document must be reviewed by PMA to which the authority is accredited and approved prior to their implementation.
Each authentication profile shall describe guidelines on identity vetting for its accredited authorities.
The issuing authority must keep records of the identity vetting process for at least three years.

3.3 Removal from the federation

Each authentication profile shall describe guidelines on removal and revocation of entities from the domain of authority.
An accredited authority may withdraw from a PMA by notifying the chair and general membership of the PMA to which it is accredited. It must observe the termination procedures described in its policy and practice statements, but it must retain the records and archives related to the identity vetting process for at least three years following the last assertion issuance.
An accredited authority may be removed from a PMA if it fails to comply with this federation document, or with the applicable authentication profile, via a qualified voting process as described in section 12.

4 Operational requirements

The federation maintains a repository and a contact electronic mail address, accessible to the general public and all relying parties alike. The federation repository shall consist of at least a public web site, with an intended continuous availability. The URL of the public web site shall be http://www.gridpma.org/.

The federation will have a secretariat role – distributed amongst its members – that will respond to inquiries in a timely manner.

Each authority within the federation shall maintain at least one contact mechanism. This mechanism must allow for un-moderated access to report problems and faults regarding the authority by the relying parties and general public. This point of contact shall be made known to the federation for subsequent re-publishing.
The authentication profile may proscribe additional operational requirements for accredited authorities under a specific AP.

5 Site security

Each accredited authority will document its site security mechanisms and this document must be made available to all direct and indirect members of the federation. Changes to this document must be reviewed by accrediting PMA and approved prior to their implementation.

This document will contain at least the software, network, server and physical security at the site of the member. It must also describe the procedural controls, personnel security controls, and the life cycle management for security controls.

The authentication profile may specify additional requirements on site security for authorities accredited under that profile. The minimum requirements on site security specified in the authentication profile will be made publicly available.

6 Publication and Repository responsibilities

The federation shall publish in its repository at least the following information*:*

- the electronic mail contact address for the federation,
- the list of its members,
- at least one contact method for each member,
- a list of assigned subject name spaces, with the associated owning authorities, by referring to the repository of the accrediting PMA
- the full texts of this federation document, and any and all of the authentication profiles in force within the federation. This shall include all versions, those currently in effect and all historical versions. An authentication profile may be managed by an assigned PMA, in which case the federation repository shall contain a link to the PMA document repository.

Each PMA shall maintain a list of its accredited authorities, the namespaces assigned to each of these authorities, and information relevant to relying parties for establishing a trust relationship with the individual accredited authorities. Within the repository of each PMA it shall be made clear under which authentication profile an authority has been accredited. Additionally, it must be possible for relying parties to select or deselect individual authorities even within a group of accredited authorities. Each PMA is only responsible for publishing information for those authorities it itself has accredited.

Each PMA shall mirror the distribution area of all PMAs that are a member of the Federation, in a single common naming scheme. *Technical details to be provided.*

Each authentication profile shall define what technical information regarding accredited authorities under that profile must be published.

7 Liability

The federation is not to be held liable for any damages, including but not limited to lost profit, lost savings and any incidental or consequential damages. The federation is not to be held legally responsible for problems arise out of its operation or the operation of any of its accredited authorities under any authentication profile, or for problems relating to the use or misuse of the assertions issued by any of its members.

Members of the federation may subsume additional liabilities if thus stated in their policy and practice documents governing that specific authority. Unless thus stated otherwise, members will not be liable for any damages.

8 Financial Responsibilities

The federation does not levy membership fees. Members are assumed to fund their own maintenance and operational costs. The cost of compliance with the federation document and the relevant authentication profile(s) is to be borne in full by the accredited authority.

In addition, each member of each of the member PMAs is expected to contribute an equal share to the continued operation of the federation by in-kind contributions, such as but not limited to the participation in the peer review process as a reviewer, and the attendance of the meetings of the federation. The IGF and the PMAs may be supported by financial grants, provided those grants benefit the operation of the federation in general and are not directed towards any authorities to fund their own operational cost.

9 Audits

The IGF and the member PMAs aim to assure that the authorities operate in accordance with this document and the authentication profile. To that end the accredited authorities must be auditable, and all authorities must keep sufficient records for a period of at least three years. The auditing requirements on accredited authorities must be described in the documents. A PMA may decide that the public availability of the results of the audit is to be limited.

10 Privacy, confidentiality

What are your privacy rules, IP policies, etc

11 Compromise and Disaster recovery

How do you handle exposed shared secrets or other compromised secrets?

12 Federation Administration

12.1 Change procedures for this federation document

This document can be changed by consensus of all participating regional and continental PMAs. In this decision the Chair represents each PMA. Each PMA must define the criterion to reach a decision on such consensus. Unless stated otherwise, this federation document will have the same status as a Charter in a regional or continental PMA.

12.2 Federation management

The federation management consists of the chairs of each of the participating regional or continental PMAs. The chairs will meet when necessary, usually by electronic means, to ensure continues operation of the federation.
Each member PMA must operate a forum in which its members convene periodically. Such a meeting will also be opened to chairs and members of any of the other PMAs. Minutes of the PMA meetings will be distributed across all members of all PMAs within the federation.

12.3 Membership applications

Each member PMA must define guidelines on membership application and on the accreditation of issuing authorities. These guidelines must contain:

- which groups and organizations can join a PMA,
- how issuing authorities are grouped by accreditation profile,
- how issuing authorities are accredited according to that profile. The accreditation shall be based on a sound review process in which the compliance of the authority with respect to this federation document and the selected authentication profile is assessed.

All accredited authorities will be members of the accrediting PMA.
Each PMA must allow representation of relying parties, and document how relying parties are represented.

12.4 Termination of membership

The members cannot withdraw from the federation. If any member decides to leave the federation the federation will cease to exist, but the other PMAs will remain.
Each PMA must describe a process by which its members can be removed from the PMA. The removal of an authority from the PMA cannot release said authority from the obligation to retain auditable records for a period of three years, not does it release it from the requirements in its own policies and practices regarding service termination of the authority. Such information must remain available to both the PMA and the federation.

12.5 Information dissemination

Each PMA will ensure that information regarding its own membership and the accreditation of authorities, as well as any changed to the charter, federation document and guidelines documents are distributed widely amongst its peers and relying parties. At least, such information is sent to the chairs or secretariats of all PMAs within the federation for forwarding to their members.