IGTF
Interoperable Global Trust Federation
AP | EU | TAG

Category: charter documents
Status: DRAFT
Document Id: FederationDocument-20140514-v2.0-03.docx
Editor: David Groep
Last updated: Thu, 05 June 2014

IGTF - Interoperable Global Trust Federation

Abstract
This document describes the constitution, policies and practices of the Interoperable Global Trust Federation, hereafter referred to as the IGTF. The goal of the IGTF is to foster harmonization and synchronization of policies and best practices to allow for global trust relationships to be established for distributed IT infrastructures for research and related purposes. The IGTF consists of three members, policy management authorities that are responsible for establishing a trust fabric in a specific geographic region: the Asia-Pacific region; Europe, the Middle East, and Africa; and in the Americas.

Table of Contents

1 Federation Definition

1.1 Description of the Federation

The Interoperable Global Trust Federation (IGTF) is a body to foster harmonization and synchronization of policies and best practices to allow for global trust relationships to be established for distributed IT infrastructures for research and related purposes. The IGTF will develop guidance and coordinate best practices in this area, including in the domain of authentication, authorization, attribute management, credential management, and operational trust.

The IGTF ensures that – within the scope of this federation document – the assertions issued by accredited authorities of any of its member PMAs meet or exceed the profiles relevant to the accredited authority.
This document is authoritative for all operations and actions of the IGTF.

1.2 Membership

The IGTF consists of the Asia Pacific Grid Policy Management Authority, the European Policy Management Authority for Grid Authentication in e-Science, and The Americas Grid Policy Management Authority. Each PMA is represented in the IGTF via its chair. By virtue of its membership of a PMA, each member of a PMA is subject to the IGTF Federation document and is thus a member of the Federation.

2 General Architecture

The IGTF – through its members – develops guidance, coordinates requirements, and harmonizes assurance levels, for the purpose for supporting trust between distributed IT infrastructures for research. This goal is accomplished by the members of the IGTF through coordination of providers of trust information (authorities) and consumers thereof (relying parties) and by adoption of common standards, minimum requirements, and best practices for policy, technical security, and operational trust.

For the purpose of establishing and maintaining an identity federation accreditation service, the IGTF maintains a set of authentication profiles (APs) that specify the policy and technical requirements for a class of identity assertions and assertion providers. The member PMAs are responsible for accrediting authorities that issue identity assertions with respect to these profiles. The PMAs do not themselves issue such assertions; the identity authorities will provide identity assertions for use in inter-organisational resource access.

For each AP, different stipulations regarding identity management, operational requirements, and site security may be in effect. The management and continued evolution of an AP is assigned by the IGTF to a specific member PMA. Proposed changes to an AP will be circulated by the chair of the PMA managing the AP to all chairs of the IGTF member PMAs. All of the PMA chairs, after approval by their PMA, are required to endorse the proposed changes before the modified AP will come into effect. The IGTF will maintain a list of supported authentication profiles and their managing PMAs in the information repository.

Each of the PMAs will accredit credential-issuing authorities and document the accreditation policy and procedures. Authorities accredited by a PMA are always subject to the policies and practices of a specific AP as determined by the accrediting PMA. The PMA's decision regarding accreditation of an authority is based on at least the (publicly available) documents describing the policies and practices of the authority. Authentication profiles will stipulate additional requirements for accreditation. Any changes to the policy and practices of a credential-issuing authority after accreditation will void the accreditation unless the changes have been approved by the accrediting PMA prior to their taking effect.

The IGTF may support and foster activities, and maintain and make available guidelines for the establishment of global trust for distributed IT infrastructures for research to support authorization,

attribute management, credential management, and collaboration on IT security issues, to the extent relevant for the member PMAs and their members.

3 Identity Federation Accreditation Service

For the purposes of establishing a globally-interoperable fabric for identity provisioning, the federation requires that every identifier issued by any accredited identity 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 all other cases, the entity must have an assigned natural person named as a responsible for this entity. This responsible person may assign or transfer responsibility for the entity to another natural person. Every accredited authority must specify a mechanism for dealing with entities whose responsible person fails in their responsibilities for an entity without assigning a new responsible for this entity.

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 the PMA member for its accredited authorities. This name space must not overlap with any existing name space already assigned to an existing PMA member for any AP, assigned by any of the regional PMAs within the IGTF.
The assignment of a name space to a PMA member will be according to current best practices, and the name space shall have a reasonable relationship to the scope of the PMA member. Any proposal for name space assignment shall be circulated amongst all PMAs within the IGTF, and the assignment will not be effective 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 the PMA to which the authority is accredited and approved prior to their implementation.
Each authentication profile shall describe guidelines on identity vetting for authorities accredited based on the profile. The issuing authority must ensure access to the records of the identity vetting process for at least three years.

4 Operational requirements

4.1 Requirements for the IGTF

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

4.2 Requirements for the member PMAs

Each PMA maintains a repository and an electronic mail address (`info@`*`pmaname`*`.org`) for inquiries by the general public. This repository shall consist of at least a public web site (`http://www.`*`pmaname`*`.org/`) with an intended continuous availability. Each PMA also provides an "announcement" mailing list to which the general public can subscribe.
In addition, each PMA shall operate a discussion mailing list or forum for use by all its members, both accredited authorities and other members, including member relying parties.

4.3 Requirements for accredited authorities

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 accrediting PMA and the IGTF for subsequent re-publishing.
The accredited authority must disclose to the accrediting PMA and to the general public its documented policies and practices.
The authentication profile may proscribe additional operational requirements for accredited authorities under a specific AP.

5 Site security

Each accredited authority will document its security mechanisms and this document must be made available to all members of the IGTF federation (i.e. all members of all PMAs). This document will contain at least the software, network, server and physical security at the site. 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

6.1 Information repository

The federation shall publish in its repository, or have published on its behalf by any of its members, at least the following information:

- the electronic mail contact address for the federation,
- the list of its member PMAs and the members of those PMAs by referring to the PMA repositories,
- at least one contact method for each member PMA,
- 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, all controlling documents, and all of the authentication profiles in force within the federation. This shall include all versions, those currently in effect and all historical versions. Each authentication profile is managed by an assigned PMA. The federation repository shall contain a link to the appropriate PMA document repository.

The URL of the public web site shall be `https://www.igtf.net/`.

Each PMA shall maintain a list of its accredited authorities, the name spaces 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.

6.2 Trust anchor distribution

Each PMA will distribute trust anchor and name space assignment information for all accredited credential-issuing identity authorities, including those accredited by other PMAs. Each PMA is only

responsible for the correctness of the information for those authorities it itself has accredited (for authorities accredited by the other PMAs the distribution will be of informational value only). Each PMA will provide information on how to validate the correctness of the published trust anchors.

The naming of the trust anchor distribution of each PMA shall be identical ("common naming"), and will contain a list of accredited authorities and a reference to the AP under which each was accredited. Additionally, it must be possible for relying parties to select or deselect individual authorities even within a group of accredited authorities.
In as far as technically feasible, the publication formats shall be common to all credential-issuing authorities, regardless of the accreditation profile under which they were accredited.

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

The IGTF will, in consultation with its members and relying parties, document the structure of the trust anchor distribution(s).

7 Liability

The Federation accepts no liability for any damages, including any incidental or consequential damages. Also, the Federation does not accept responsibility for problems arising 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. Unless 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 regional PMA. The IGTF 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 operational cost.

9 Audits

The IGTF and the member PMAs aim to assure that the authorities operate in accordance with this document and the relevant authentication profile(s). 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 IGTF documents. A PMA may decide that the public availability of the results of the audit is to be limited.

10 Privacy and Confidentiality

All information provided to the IGTF should be regarded as confidential information unless noted otherwise. This document, the authentication profiles, the PMA membership lists and list of accredited authorities, trust anchor distributions, PMA guideline documents, and all announcements and informational messages intentionally distributed to the general audience are public information. Each PMA can classify information at its discretion.

11 Compromise and Disaster recovery

Any suspected compromise or disaster should be made known to the IGTF, the PMA or to the authority involved, as applicable. To this end, an electronic mail address of the form `concerns@`*`pmaname`*`.org` and the address `concerns@igtf.net` will be made available.

11.1 Compromise of an IGTF or PMA repository

If a repository of trust anchor distribution location of either the IGTF or any of its member PMAs is compromised, it hosting system(s) will be quarantined and the incident investigated according to current best practice. Pending the investigation, a replacement will be provided as soon as practical. Wide notice of this event will be sent to all members, relying parties and the general public. After investigation, a full report and damage assessment will be made available to the PMA chairs and abstracts will be made available to the PMA membership, relying parties and the general public.
It should be noted that the IGTF and PMA repositories are not to be used as time-critical components by any third party, since continuous availability is explicitly not guaranteed.

11.2 Compromise of a credential-issuing authority

Each authority must define a compromise and disaster recovery procedure, and be willing to discuss the procedure within the accrediting PMA. Authentication profiles may set specific requirements for such procedures.

12 Federation Administration

12.1 Change procedures for this federation document

This document can be changed by consensus of all members. 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 member 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, possibly by electronic means, to ensure continued operation of the federation.
The IGTF itself will have a chair. The role of chair of the IGTF will be filled by one of the regional PMA chairs. This role will last for one year and will be rotated to the other PMA chairs on the anniversary of the founding of the IGTF, from Europe to the Asia-Pacific to the Americas and then to Europe again.
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.
The IGTF can develop other controlling documents as needed.

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 Dispute resolution

Disputes may be brought to the attention of the IGTF or to any of the member PMAs by sending an electronic mail message to the “concerns” address of the relevant body. Whenever possible, disputes will be resolved by the PMA whom the issue concerns. The PMA chairs will resolve IGTF-related disputes via unanimous decision.

12.5 Termination of membership

If any member decides to leave the federation the federation will cease to exist, but the individual PMAs will remain to exist.

An accredited authority or member may withdraw from a PMA by notifying the chair and general membership of the PMA to which it is accredited. It is assumed that a credential-issuing authority that withdraws from the federation will continue to observe the procedures described in its own policy and practice statements. In particular it should retain the records and archives related to the identity vetting process as mentioned in section 3.2.
An accredited authority may be removed from a PMA if it fails to comply with this federation document, or with the applicable authentication profile. The proposal for removal is subject to a qualified voting process unless the PMA has itself described a removal procedure in its own charter or bylaws. The removal of an authority from a PMA must be announced widely by that PMA to the membership of all the PMAs and to the community and relying parties in as far as possible.

Each authentication profile shall describe guidelines on removal and revocation of entities within each individual domain of authority.

12.6 Information dissemination

Each PMA will ensure that information regarding its own membership and the accreditation of authorities, as well as any changes 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.

Copyright Notice