GFD-I
Category: Informational Documents
CA Operations WG

Tony J. Genovese, ESnet/LBL
David Groep, NIKHEF
Christos Kanellopoulos. AUTH
September 13, 2006

# Guidelines for Authentication Service Profiles for Grids

## Status of This Memo

This memo provides information to the Grid community regarding Authentication federations being deployed by Grids. It does not define any standards or technical recommendations. Distribution is unlimited.

## Copyright Notice



## Abstract

The international scientific community is deploying computational Grids for the advancement of science and engineering. The promise of global computational Grids requires policies and procedures that reliably identify Grid subscribers and resources. The utilization of Grids today depends on trusted Identity Providers (IdPs). Grid IdPs are responsible for issuing Authentication tokens to individuals and Grid resources. An IdP loosely consists of:

- At least one Authentication Service that complies to a specific IGTF [www.GridPMA.org] Authentication Service Profile
- A governing board to manage policies and trust relationships
- Set of membership and accreditation procedures
- Operational requirements for the service
- Information publishing process

In this paper we focus on the requirements for defining an Authentication Service Profile that can be used by IdPs to provide compliant Authentication Services. The other components that are required by an Identity provider are not covered.

The purpose of this document is to provide Identity providers with a guideline for defining and publishing an Authentication Service Profile. There will be one profile for every accredited Authentication Service type deployed in the Grid community. The use of the profile will ensure that independent IdPs implementing a particular Authentication Service Profile type will provide comparable service to their individual communities.

An Authentication Service Profile provides a way for Grid Relying Parties (RP) to be able to identify and compare Authentication Services provided by Identity Providers. An IdP can provide Authentication Services based upon one or more Authentication Service Profiles. Currently the IGTF has identified a number of Authentication Service Profiles being researched or deployed by Grid Identity providers:

1. Classic PKI
2. Short lived credential services

Tony J. Genovese, ESnet/LBL
David Groep, NIKHEF
Christos Kanellopoulos. AUTH


3. Large site integrated proxy services (SIPS)
4. X.509 credential repositories – active credential stores (ACS)
5. Non-PKI based Authentication (i.e. Kerberos, One Time Passwords, etc)
6. Member integrated Certificate service (MICS)

Tony J. Genovese, ESnet/LBL
David Groep, NIKHEF
Christos Kanellopoulos. AUTH



# Table of Contents

1. Introduction ..... 4
1.1 Support documents ..... 4
2. Grid Identity providers (IdP) ..... 4
3. Authentication Federation ..... 5
4. Authentication Service Profile ..... 5
4.1 Authentication Service management ..... 6
4.2 General Architecture ..... 6
4.3 Identities (person, host, service identities) ..... 6
4.4 Operational requirements ..... 6
4.5 Facility security ..... 6
4.6 Publication and Repository responsibilities ..... 6
4.7 Liability ..... 6
4.8 Financial Responsibilities ..... 6
4.9 Audits ..... 7
4.10 Privacy, confidentiality ..... 7
4.11 Compromise and Disaster recover. ..... 7
5. Examples of Authentication Service profiles ..... 7
6. Intellectual Property Statement ..... 7
7. Full Copyright Notice ..... 7
8. References ..... 8

# 1. Introduction

For an Authentication Service to be trusted by relying partners a level of trust has to be established in the Identity provider. The relying parities are concerned with controlling access to their resources by participants that may or may not be local or even a member of their community. To facilitate global access, but maintain local control, the Grid community has split the Authentication and Authorization processes. The Grid community has a number of Identity providers organized as Federations around the world, which provide high quality identity tokens for use by relying parties. The Authorization step is completely left to the control of the relying party and this paper will not address Authorization issues.

We introduce two terms that are used by Grids to address Grid Authentication. They are ***Grid Identity provider*** and ***Authentication Federation***. These terms will be discussed below.

In this paper we focus on the requirements for defining an Authentication Service Profile that can be used by IdPs to provide compliant and trusted Authentication Services. An Authentication Service Profile provides a way for Grid Relying Parties (RP) to be able to identify and compare Authentication Services offered by independent Identity Providers.

## 1.1 Support documents

A number of documents have been written that help IdPs and their Federations. In PKI based Identity providers, RFC 3647 can be used to specify the operational and policies needed to manage the IdP [RFC3647]. The US government has also produced a guide for use by its agencies to set up a X.509 based authentication [FBCA]. In addition to these documents the GGF has produced guides to facilitate management of the IdP and its federation.

1. Policy Management Charter [GFD.62]: This document provides guidelines to charter and manage the governing board of the Federation
2. Global Grid Forum Certificate Policy model [GFD16]: This document can be used by PKI based Authentication Services to define the policy and procedures used by the service

# 2. Grid Identity providers (IdP)

***A Grid identity provider is defined:*** As an individual or group that has permission of a community to manage and operate a service whose purpose is to issue identity tokens to Grid users or Grid services. This service to the Grid community is called an Authentication Service. Each Authentication Service is based on one an only one Authentication Service Profile. A Grid identity Provider may offer more then one Authentication service.

A Grid IdP consists of more than the Authentication Service it offers its community. It must be governed by a management board, which will establish policies and procedures under which it will operate. A Grid IdP must operate the Authentication Services to some consistent and auditable set of requirements that are defined in an Authentication Service Profile and it must have a publishing site that both existing and potential future members can access and review. An IdP loosely consists of:

- At least one Authentication Service that complies to a specific IGTF [www.GridPMA.org] Authentication Service Profile
- A governing board to manage policies and trust relationships
- Set of membership and accreditation procedures
- Operational requirements for the service
- Information publishing process

An IdP can provide Authentication Services based upon one or more Authentication Service Profiles. Currently the IGTF has identified a number of Authentication Service Profiles being researched or deployed by Grid Identity providers:

1. Classic PKI
2. Short lived credential services
3. Large site integrated proxy services (SIPS)
4. X.509 credential repositories – active credential stores (ACS)
5. Non-PKI based Authentication (i.e. Kerberos, One Time Passwords, etc
6. Member integrated Certificate service (MICS)

## 3. Authentication Federation

***An Authentication Federation is defined:*** As two or more IdPs that agree to work together to provide a common service to their communities. This federation should include the IdPs relying parties. This federation will be responsible for accrediting member IdPs and the service they offer.

The federation has responsibilities similar to that of an independent IdP. It must be governed by a management board, which will establish policies and procedures under which it will operate. An Authentication Federation's members must operate the Authentication Services to some consistent and auditable set of requirements that are defined in an Authentication Service Profile. It must have an information publishing site that RPs; existing and future members can access and review. An Authentication Federation loosely consists of:

- Two or more IdPs
- At least one Authentication Service that complies to a specific Authentication Service Profile
- A governing board to manage policies and trust relationships
- Set of membership and accreditation procedures
- Operational requirements for the service
- An information publishing process

## 4. Authentication Service Profile

An Authentication Service Profile is used to specify the requirements for operating a particular type of authentication service. In PKI based systems these technical details are provided by the Certificate Profile (CP) and the Certification Practice Statement (CPS). In the case of a PKI based authentication service, the PKI Authentication Service Profile would specify specific requirements that must be implemented in the CP/CPS of the provider. This way independent PKI based identity providers that wish to work together can develop a common profile for their type of service.

A survey of current IdPs and their RPs point to a common set of topics all successful services have. This list will be the bases for what is included in an Authentication Service Profile

1. Describe who is responsible for providing the service
2. Description of the General Architecture
3. Describe how Identity is assigned
4. Specify Operational requirements for computational and human elements
5. Describe Site security
6. Publication and Repository responsibilities
7. Liability
8. Financial responsibilities
9. Audits
10. Privacy and confidentiality
11. Compromise and disaster recovery.

The following sections describe the main areas each Authentication Service Profile should address. The Authentication Service Profile can consist of one or more documents, but all of the following sections should be addressed. It is recommended that each Identity provider start with one document that contains all the following sections. If an Authentication service specification is complex the primary service description document will include pointers to external documents. The goal is to have one primary document that specifies the Authentication service to aid in relying parties review. The content in each of the following sections are suggestions for content

or questions that should be address. Your Authentication service will adjust the content as needed. The structure must be preserved for consistency and ease of review for our relying parties.

## 4.1 Authentication Service management

- Describe who is responsible for the service and change control.
- Specify the community that will be served by the Authentication Service.
- Specify the scope of the service.

## 4.2 General Architecture

- Describe the system architecture used to build the authentication service used by the Identity provider. How does the customer and management interface to the system?

## 4.3 Identities (person, host, service identities)

- The Authentication service must describe how identity is managed and communicated in the community.
- Each Authentication service must define Identity vetting rules, what each user does to prove the identity of the user, host or service identified as part of an organization.
- Identity revocation: how a person or system is removed from the service.
- Is there a special Acceptable Use Policy that applies?

## 4.4 Operational requirements

- QOS for the authentication service: is 24/7 support or not?
- Trouble ticket reporting and tracking system.
- Information request and general customer support.
- Required contact information, problem reporting/resolution procedures.

## 4.5 Facility security

- For each authentication service used by the identity service provider describe the: Software, network, server and physical security at the site of the authentication service.
- Also describe: procedural controls, personnel security controls. Life cycle for security controls - How do you update/change security controls and keep the community informed?

## 4.6 Publication and Repository responsibilities

- What information must be published and maintained by the Authentication service?
- How long must information be maintained?
- Access rights to read or use the information.

## 4.7 Liability

- What liability or warranties are supported by the service?

## 4.8 Financial Responsibilities

- How do you pay for the service?

- Any financial responsibilities to your members?

### 4.9 Audits

- Do you audit each authentication service for compliance to your policies?
- Do you conduct self audits or member audits or open to external audits.
- What access to the results of the audit is allowed?

### 4.10 Privacy, confidentiality

- What are your privacy rules, IP policies, etc?

### 4.11 Compromise and Disaster recover.

- How do you handle exposed shared secrets or other compromised secrets?
- What facilities are in place to rebuild the service if there is a disaster?
- How long would the service be out of commission if the service is compromised or damaged?

## 5. Examples of Authentication Service profiles

Check the International Grid Trust federation (www.GridPMA.org) site for Authentication Service profiles that have been specified or under development.

## 6. Intellectual Property Statement

The GGF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the GGF Secretariat.

The GGF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this recommendation. Please address the information to the GGF Executive Director.

## 7. Full Copyright Notice

GGF Document process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the GGF or its successors or assigns.



## 8. References

[FBCA] - X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA), Version 1.0, 18 December 1999

[GFD16] – Global Grid Forum Certificate Policy Model, Randy Butler, Tony Genovese, June 2003

[GFD62] – R. Cowles, T. Genovese, P. Gietz, M. Helm, Policy Management Authority Model Charter, January, 2006

[RFC3647] - S. Chokani and W. Ford, Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework, RFC3647 (obsoletes 2527), November 2003