Tony J. Genovese, ESnet/LBL

Guidelines for Authentication Federations in 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

Copyright © Global Grid Forum (2005). All Rights Reserved.

Abstract

To facilitate deployment of Grid Computing and to allow for innovation with respect to Authentication Services we have developed a method to define and publish Authentication Federations. An Authentication Federation provides a way for Grid relying parties to be able to identify and compare Authentication Federations that are being deployed to support Grids. Currently we have identified five classes of Authentication Federations being researched or deployed to support Grids.

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

In this paper we outline what is needed to build trust in a Grid Authentication Federations. As new technologies or services are deployed, they can make use of the guidelines described in this paper to publish their Authentication Federation specification. The users of this service can have access to all pertinent information to determine trust. Currently there are a number of successful Grid Authentication Federations based on PKI that have been deployed.

Tony J. Genovese, ESnet/LBL

Table of Contents

1. Introduction

Authentication Federations consist of an authentication service (i.e. PKI, Kerberos, etc), the management and operational process for the service and the community it serves. As we deploy our Authentication Federations in support of Computing Grids we need to provide the relying parties a way to evaluate these federations for trust. Currently the most prevalent solutions for authentication used by Grids are based on PKI. This is not to say that other methods will not be developed. This paper is to address how to identify and publish these Authentication Federations to allow for concise and consistent review by our relying parties.

To facilitate deployment of Grid Computing and to allow for innovation we have specified a method to define and publish the various Authentication Federations being deployed by Grids. An Authentication Federation is designed to provide all the information a Grid relying party needs to be able it identify and compare different Authentication Federations. Currently we have identified five classes of Authentication Federations being researched or deployed to support Grids.

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

In this paper we develop what is need to build trust in a Grid Authentication Federation. As new technologies or services are deployed, they can make use of the guidelines described in this paper to publish their Authentication Federation. The relying parties of this service can have access to all pertinent information to be able to determine trust.

2. Authentication Federation

In the Grid today there are a number of Authentication Federations being deployed in support of Grid computing. The purpose of this document is to provide a guideline for defining and publishing an Authentication Federation. The Authentication Federations in Grids are based primarily on PKI, this does not preclude other technologies from being defined and deployed. The inclusion in this document and the publishing of a Federation does not imply a warranty or the appropriateness of a published Federation. The decision to trust the published authentication Federation can only be made by a relying party.

2.1 What needs to be specified in an Authentication Federation?

For an Authentication Federation to be trusted by relying partners a level of trust has to be established and maintained. The relying parities are concerned with controlling access to their resources by participants that 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 authentication service 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. To build trust in their authentication services the community has been providing the following basic services:

1. A governing board to manage the authentication service or service providers.
2. Set of membership and accreditation procedures.
3. Operational requirements for the authentication service or services.
4. A publishing process for operational information and trust anchors that relying parties can trust.

2.2 Federation document

This section covers an outline for the controlling document of an Authentication Federation. It establishes the structure and responsibilities of its members. The content of this outline is based on the successful deployment of grid federations like WWW.EUGridPMA.org. WWW.APGridPMA.org, WWW.TAGPMA.org and WWW.GridPMA.org. The outline identifies the 12 areas that must be addressed by every federation. This outline can be use to specify:

1. A federation describing an Authentication Service
2. A federation of people or institutions using Authentication Services
3. A federation of federations

In PKI based Authentication Federations, RFC 3647 and its related documents can be used to define the operational and policies needed to manage the Federation [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 federation.

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

It is recommended for all Authentication services, even PKI based services that they use this federation document to manage their federation. In the federation document for PKI based authentication services, there would be pointers to the external specifications (i.e. CP/CPS, PMA charters).

2.2.1 General Federation Document outline

The following outline describes the main areas each authentication federation should address in its Federation document. The federation specification can consist of one or more documents, but all of the following sections should be addressed. It is recommended that each federation start with one document that contains all the following sections. If a Federations' specification is complex the primary federation document will include pointers to external documents. The goal is to have one primary document that specifies the federation 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 federation will adjust the content as needed. The structure must be preserved for consistency and ease of review for our relying parties.

2.2.1.1 Federation definition

- Describe its mission.
- Specify the community that will be served by the federation.
- Specify the scope of the federation
- What activities are included or excluded by the federation
- If the federation will be chartering itself, specify the founding members and in the Administrative section how they vote on the charter.

2.2.1.2 General Architecture

- Describe the system architecture used to build the authentication service used by the federation.
- If this is a federation of sites/people, what are their relationships to each other?

2.2.1.3 Identity service (person, host, service)

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

2.2.1.4 Operational requirements

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

2.2.1.5 Facility security

- For each authentication service used by the federation 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?

2.2.1.6 Publication and Repository responsibilities

- What information each federation must publish and maintain.
- How long information must be maintained?

2.2.1.7 Liability

- What are you liable for or NOT.

2.2.1.8 Financial Responsibilities

- How do you pay for the service?
- Any financial responsibilities to your members?

2.2.1.9 Audits

- Do you audit each authentication service for compliance to your policies or do you trust each provider? Self audits or member audits or open to external audits by members only...

2.2.1.10 Privacy, confidentiality

- What are your privacy rules, IP policies, etc

2.2.1.11 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?

2.2.1.12 Federation Administration

- The federation charter can point to an external document based on the GGF PMA charter to define the management of the federation.

The Administration section of the federation document describes how the federation is managed. This usually requires the establishment of a board to over see the federation documents and operations. The federation if small could be managed by an individual, but it is assumed that the federation will be large and use a board of directors to manage it. This board is the responsible agent for management and control of the federation. The following sections should be included in the administration section of the federation document:

1. Introduction - federation board description
2. Scope
    a. Included activities
    b. Excluded activities
    c. Change procedures for this federation document
    d. Change control for other documents used
    e. Peering with other federations
    f. Territory/area covered by federation
    g. Accreditation of Authentication Service providers
    h. Dispute resolution – customers and members.
3. Chartering procedure or process
    a. What is the procedure to establish the federation?
    b. Are there founding members
    c. Federations can be organized as self chartering Permanent Societies.
4. Membership
    a. Description of Officers/Roles and general membership
    b. Must define Chair Role
    c. May define Secretary role
    d. May define Security Officer role
    e. May define liaisons to other federations
    f. New or renewing membership process
    g. All roles and memberships should have term limits
    h. Resignation/Expulsion rules
    i. How does an authentication service join the federation?
    j. How does an authentication service leave the federation?
5. Governance
    a. Meetings – when and how are they scheduled, quorum requirements
    b. Voting process
    c. How do you exchange information with each member in a secure manner?

3. Federation authentication service publication requirements

A Grid Authentication Federation will consist of one or more authentication services. Each Grid authentication service must have a well know publishing point for information used by the relying parties. There is no single publishing point that relying parties can go to find a Grid authentication services. Some of the information that relying parties will need in a Grid authentication service is:

1. Contact for the federation administration
2. Access to published documents of the authentication service.
3. For PKI based systems a trusted independent source for trust anchors.
4. Contact for reporting problems or requesting customer assistance.

A common publishing point for Grid authentication services would facilitate Relying parties locating the needed information. It is recommended for Grid authentication services that the above information be published in a GGF Informational doc and published by the GGF. This will provide a common publishing location for Grid authentication providers.

4. Example Grid Federations

The following are links to federations that have used this document.

The International Grid Trust Federation www.GridPMA.org
Federation document: http://eugridpma.org/igf/IGF-Federation-20050525-0-3.doc

The Americas Grid PMA www.TAGPMA.org
Federation document: http://www.gridpma.org/docs/TAGPMA%20charter%20v1.pdf

5. 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.

6. Full Copyright Notice

Copyright (C) Global Grid Forum (date). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the GGF or other organizations, except as needed for the purpose of developing Grid Recommendations in which case the procedures for copyrights defined in the 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.

This document and the information contained herein is provided on an "AS IS" basis and THE GLOBAL GRID FORUM DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE."

7. 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

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