

Grid Authentication profiles

Status of This Memo

This memo provides information to the Grid community regarding the profiling of the various types of PKIs being deployed by Grids. It does not define any standards or technical recommendations. Distribution is unlimited.

Copyright Notice

Copyright © Global Grid Forum (2004). All Rights Reserved.

Abstract

In the deployment of Grid computing we have chosen to primarily use Public Key Infrastructure to support distributed identity authentication. This technology is undergoing expansion and innovation. To facilitate deployment of Grid Computing and to allow for innovation we have defined a method to define and publish the various authentication profiles being deployed by Grids today. An Authentication Profile is designed to provide a way for a Grid relying parties to be able to identify and compare like Authentication services that are being deployed to support Grids. Currently we have identified three types of PKIs being deployed to support Grids today.

1. Classic PKI infrastructures
2. Large site integrated proxy services (SIPS)
3. X.509 credential repositories

In this paper we explore what is need to build trust in a Grid Authentication service. There are a number of successful Grid Authentication services based on PKI that have been deployed. They are shown as examples of what has worked in the community.

Table of Contents

1.	Introduction	3
2.	Authentication profiles	3
2.1	What needs to be in an Authentication profile?	3
3.	Managing a Authentication service.....	3
4.	Establishing membership and operational requirements	4
5.	Authentication service publication requirements	4
6.	Example Authentication service profiles.....	4
	Intellectual Property Statement	4
	Full Copyright Notice	4
	References	5

1. Introduction

As we deploy authentication mechanisms in support of Computing Grids around the world we need to provide the relying parties a way to evaluate these services. 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 services for review of the relying parties that have to trust the method of identity proofing.

To facilitate deployment of Grid Computing and to allow for innovation we have defined a method to define and publish the various authentication profiles being deployed by Grids today. A PKI Profile is designed to provide a way for a Grid relying parties to be able to identify and compare similar PKIs that are being deployed to support Grids. Currently we have identified three types of PKIs being deployed to support Grids today.

1. Classic PKI infrastructures
2. Large site integrated proxy services (SIPS)
3. X.509 credential repositories

In this paper we will identify the current set of PKIs being deployed in Grids today. It will describe a publishing method for these PKIs to register their individual PKI profiles and make them available to their relying parties.

2. Authentication profiles

Currently there are 3 types of PKI being deployed in support of Grid authentication. The purpose of this document is to provide a tool for registering and publishing an Authentication profile. Though this document reflects the current state of Authentication in Grids, based on PKI, this does not preclude other technologies from being defined and deployed. The inclusion in this document and the publishing of a profile does not imply a warranty or the appropriateness of a published profile. The decision to trust the published authentication method can only be made by a relying party.

2.1 What needs to be in an Authentication profile?

Using our experience over the past couple of years in deploying Grid PKIs, we have discovered a basic set of operational requirements for identity providers. For a PKI to be trusted by relying partners a level of trust had to be established and maintained. The relying parties 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 community has split the Authentication and Authorization processes. The Grid community has a number of Authentication providers around the world, which provide high quality identity tokens for use by relying parties. The Authorization step is completely left in the control of the relying party. To build trust in their identity services the community has been providing the following basic services:

1. A governing board to manage the Authentication service
2. Set of membership and operational requirements
3. A publishing method for operational information.

3. Managing a Authentication service

The technologies used by Grid PKIs are readily available and can be run or operated by anyone. In fact the relying parties would be a good source for Authentication services, but this would lead to a proliferation of Authentication providers with out developing a high level of mutual trust. To build an authentication service that multiple relying parties can use a few large scale PKIs have been established. One of the common characteristics that these PKIs have is that each is managed by a profession board of directors. These boards or Policy Management Authorities have responsibility to manage the Authentication service and the relationship with the relying parties.

To help in the formation of these PMAs the Global Grid Forum has produced an informational document that describes how to setup and manage a PMA [*PMA reference doc*].

The PMA and the operational Authentication service it manages is what the relying parties must depend on. The quality and history of the PMA management and operations will help establish the relying parties trust in the Authentication service being provided.

4. Establishing membership and operational requirements

One of the requirements of the PMA is to establish membership rules and minimum operational requirements. This is spelled out in the PMA charter that the PMA operates under. This charter can be reviewed by the Relying parties for transparency and for potential problem resolution. The operational requirements that are established by the PMA will be the bases for review of trust by the relying parties.

5. Authentication service publication requirements

Each successful Authentication service has a well know publishing point for information used by the relying parties. Some of the information that relying parties will need in a Grid PKI based authentication service is:

1. Contact for the PMA
2. Access to published documents of the Authentication service.
3. Trusted independent source for trust anchors.
4. Contact for reporting problems or requesting customer assistance.

6. Example Authentication service profiles

Maybe do this as an appendix... Add EU, DOEGrids and AP as examples of Classic PKI profiles. We could use FNAL as a SIPS... We can add NERSC, possible credential store.

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.

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."

References