GWD-I
Category: Informational
GGF Working Group on
Authorization Frameworks and Mechanisms

Markus Lorch, Virginia Tech
Dane Skow, Fermi National Accelerator Laboratory

2004-01-23

GGF DOCUMENT SUBMISSION CHECKLIST (include as front page of submission)	
	COMPLETED (X) - Date
1. Author name(s), institution(s), and contact information	(X) – 2004-01-23
2. Date (original and, where applicable, latest revision date)	(X) – 2004-01-23
3. Title, table of contents, clearly numbered sections	(X) – 2004-01-23
4. Security Considerations section	(X) – 2004-01-23
5. GGF Copyright statement inserted (See below)	(X) – 2004-01-23
6. GGF Intellectual Property statement inserted. (See below) NOTE that authors should read the statement.	(X) – 2004-01-23
7. Document format - The GGF document format to be used for both GWD's and GFD's is available in MSWord, RTF, and PDF formats. (note that font type is not part of the requirement, however authors should avoid font sizes smaller than 10pt).	(X) – 2004-01-23

GWD-I
Category: Informational
GGF Working Group on
Authorization Frameworks and Mechanisms
2004-01-23

Markus Lorch, Virginia Tech
Dane Skow, Fermi National Accelerator Laboratory

Authorization Glossary

Status of This Memo

This memo provides information to the Grid community in the area of Grid authorization. It does not define any standards or technical recommendations. Distribution is unlimited.

Copyright Notice

Abstract

This document provides a comprehensive glossary for the area of grid authorization.

Contents

1. Introduction

This document provides a comprehensive glossary for the area of grid authorization. An attempt has been made to identify the most common interpretation of the terms while also pointing out possible alternatives in various contexts. The reader is asked to verify the applicable definition for the context in question.

2. Glossary

AAA (Authentication, Authorization, Accounting) Server RFC 2904

Access Control Decision Function (ADF) ISO-1011813, 3.2
Makes authorization decisions about a subject's access to a service. It is equivalent to the **Policy Decision Point (PDP)** defined in RFC2904. It is normally part of an Authorization server and is independent of the Resource or Application. However, it may be co-located with the Access Control Enforcement Function.

Access Control Enforcement Function (AEF) ISO-1011813, 3.2
Mediates access to a resource based on authorizations decisions by an Access Control Decision Function (ADF) or service. It is equivalent to the **Policy Enforcement Point (PEP)** defined in RFC2904. It is most often either integrated into or located in front of the resource it protects.

Access Policy < equivalenced to Policy in 4.3 >
The list of rules in a particular expression language which govern whether or not requests for access will be approved.

Administrative Domain (2.3)
Those machines and services administered by the same organization. Alternately, those machines and services which are subject to the same operational rules.

Assertion (4.1.1)

Attribute (3.3), (4.1.1), 4.2.3.1

Attribute Acquisition RFC 3281, 3.3

Attribute Application RFC 3281, 3.3

Attribute Assertion (3.4.1), 4.2.3

Attribute Authority 2.1, 4.1.1

Attribute Certificate (3.4.1)
An X.509 attribute certificate as defined in RFC 3281 by the IETF.
One type of Attribute Token.
[RFC2904 -- structure containing authorization attributes which is digitally signed using public key cryptography.]

Attribute Domain (4.2.1)
The domain in which attributes are understood to have the same meaning ?
The domain across which a given Attribute Authority is recognized as the authority ?

Attribute Repository 4.2.3.2

Attribute Schema (4.2.3.1)
The schema for describing the meaning and structure of an attribute and its elements

Attribute Token (4.2.3.2)
The object which is presented as proof of right to claim an attribute.

Authentication Credential (4.4)
Those pieces of information necessary for some entity to authenticate as a given identity. Includes an identifier (eg. a username) and some secret (eg. a password).

Authentication Token (4.2)
The object which is presented as proof of having authenticated to the issuer of the token.

Authority (2.1)
Typically an authority is some entity asked to make some decision or create some token and is given the franchise to do so by some source of authority. That franchise may be given by previous agreement, some chain of delegation, or a trust on the part of the relying party.

Authority Policy (4.2.1)
The policy which determines which authorities are accepted and how the franchises are granted.

Authorization (AuthZ) 2.0

Authorization Agent Sequence 2.2.3

Authorization Algorithm 4.5

Authorization Architecture 3.1

Authorization Assertion 4.2

Authorization Attribute 4.2

Authorization Context 4.4

Authorization Credential (4.4)

Authorization Decision (2.0.3)
The decision on what type of authorization is granted. Often this is a logical return (yes, no, indetermined) and an authorization token.

Authorization Information (2.1)
The information presented with the authorization request trying to persuade the authority to grant the authorization.

Authorization Policy (2.1), (4.4)
[Is this the same as Access Policy ?]

Authorization Privileges (4.4)
[Is this a synonym for privilege ? Is there any other type ?]

Authorization Pull Sequence 2.2.2

Authorization Push Sequence 2.2.1

Authorization Request (3.4.2), (4.4)

Authorization Response (3.4.2), 4.5

Authorization Sequence RFC 2904 (2.2)

Authorization Server 2.1, 4.2.1, 4.5

Authorization Subject 2.1

Authorization System (3.1)
One particular implementation of an authorization sequence/model. It might refer to a placeholder for one implementation (eg. on an architectural diagram). Includes all the processes, procedures and protocols necessary to carry out an authorization for that particular implementation.

Authorization Token 2.0.2

Certification Authorities (CA) 2.1

Community Domain (2.3)

Delegation Attribute (4.2.3)
An attribute expressing an authorization for the subject to carry out certain actions on behalf of the issuer.
Or rather: An attribute which transfers to the subject some authorization held by the issuer.
Or: An attribute authorizing the subject to assert some right claimed by the issuer.

Domain (2.3)

Enforcement of access rights 4.6

Environmental Authority 4.1.1

Holding Subjects (3.4.1)

Home Domain (2.3)

Identity Token (4.2.3.3)
<Is this equivalent to a Certificate for our uses ?>

Object System (3.4.3.4)

Parameters (3.3)

Policy (3.3), (3.4.3), (4.1.1), 4.2

Policy is a very broad term that needs to be constrained. In the general security context policy may cover things outside of the authorization domain, such as standards for message security, user identification, document encryption requirements, etc. Policy in the authorization domain (aka authorization or access-control policy) is typically limited to information about resource access (see Authorization Policy)

Policy Authority 2.1, 4.1.1

Policy Decision Point (PDP) RFC 2904, 3.2
The point where policy decisions are made, see Access Control Decision Function

Policy Enforcement Point (PEP) RFC 2904, 3.2
The point where the policy decisions are actually enforced, see Access Control Enforcement Function

Policy Statement 4.5

Policy System (Fig. 3-2)

Privelege 4.2

Privelege Assignment 4.2.2

Privelege Authority 4.2.1

Privelege Management 4.1, 4.2

Proxy (4.1.2)

Resource 2.1

Resource Authority 4.1.1

Rights (2.1)

Service (2.0)

Service Point (2.0)

Service Provider RFC 2904

Source of Authority (SOA) 4.1.1

Subject 2.1

Subject Attributes 3.4.1

Subject Domain (4.2.1)

System (3.4.3)

Transport Channel (4.4)

Trust (4.1)

Trust Authorities (4.1.1)

Trust Management 4.1

Trust Relationship (2.5), (4.1.1)

Untrusted Services (4.6.2)

User RFC 2904 (2.2)
the entity seeking authorization to use a resource or a service.

User Home Organization RFC 2904 (2.2)

Virtual Organization Domain 2.3

Wire Format [System] (3.4.3.4)

X.509 (4.2)
ITU-T Recommendation X.509 (1997 E): Information
Technology - Open Systems Interconnection - The
Directory: Authentication Framework, June 1997.

X.509 Certificate (ref RFC 2459 ?) (4.2.3.3)

s-expression (3.4.3.1)

3. Expansion of Acronyms:

AAA - Authentication, Authorization, Accounting
ACL - Access Control List (4.3)
API - Application Programming Interface (3.4.3.5)
WS-* Standard (3.4.3.5) { I believe this should be spelled out referencing the body of standards referenced }
QoP (3.4.3.5)
NIS - Network Information Service (?) (4.1.1)
OGSA - Open Grid Services Architecture (ref >>>) (3.4.3.5)
PKI - Public Key Infrastructure (4.1.1)
POSIX (4.6.2)
RBAC - Role Based Authorization Control (?) (4.1)
SAML - Security Assertion Markup Language (ref >>>>) (3.4.3.5)
SAML-P (4.6)
SSL - Secure Socket Layer (4.1.1)
Virtual Organization (VO) (2.3)
WS-Policy (3.4.3.5)
WS-Security - Web Services Security (ref >>>>) (3.4.3.5)
WSDL - Web Services Description Language (3.4.3.5)
XACML (3.4.3.5)
XML - eXchange Markup Language (ref XXXX) (3.4.3.1)

4. Security Considerations

While this document defines the general meaning and semantics of technical terms used by the GGF community for the area of grid authorization it may be that specific systems attach different semantics to these terms. It is thus important to verify the exact meaning of terms used in a specific system before making security critical decisions based on the interpretation. This may be especially important for authorization decision functions that interpret authorization attributes.

Author Information

Markus Lorch
Department of Computer Science
Virginia Tech (m/c 106)
Blacksburg, VA 24061, USA
email: mlorch@vt.edu

Dane Skow
Fermi National Accelerator Laboratory
MS 369
P.O. Box 500
Batavia, IL 60510-0500
email: dane@fnal.gov

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

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