Markus Lorch, Virginia Tech
Dane Skow, Fermi National Accelerator Laboratory
Mary Thompson, Lawrence Berkeley Nat'l Laboratory

GGF DOCUMENT SUBMISSION CHECKLIST (include as front page of submission)	
	COMPLETED (X) - Date
1. Author name(s), institution(s), and contact information	(X) – 2004-02-24
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

Markus Lorch, Virginia Tech
Dane Skow, Fermi National Accelerator Laboratory
Mary Thompson, Lawrence Berkeley Nat'l 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.

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 should use the applicable definition for the context in question. When the term is defined in a standards document, that document is referenced. The numbers in parentheses refer to paragraphs in the GGF document "Conceptual Grid Authorization Framework and Classification" which is an informational document that intends to introduce the vocabulary and models for Grid authorization.

Highlighted terms do not appear in the Authorization Framework, but are used in the OGSA authorization documents.

2. Glossary

AAA (Authentication, Authorization, Accounting) Server RFC 2904
A server that handles authentication of users, authorization of users to access resources, and accounting of the use of the resources. Often these functions are handled by three separate servers.

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 authorization 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 (4.2,4.3)
The list of rules in a particular expression language which govern whether or not requests for access will be approved. Also called authorization policy.

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 and accept the same source of authority.

Assertion (1.2, 4.1.1)
A statement by some authority that a subject has some property. The authority may be explicitly named in the assertion, or may be implied by the source of the assertion. See attribute and authorization assertions.

Attribute (3.3, 4.1.1, 4.2.3.1)
A named property and value associated with an entity. The most commonly used attributes are those associated with subjects, .e.g., roles, group membership or privileges. Attributes can also be associated with resources, such as the clearance level required to access the resource

Attribute Assertion (2.1, 4.2.3.3)

A statement that a subject (i.e. the holder of the attribute) has a given property. In some cases the property has a single value, e.g. “Is a faculty member”. In other cases, it is a name/value pair, e.g. role=administrator. In the case of a privilege assertion it consists of allowed action and a resource name. The statement is made by an attribute or privilege authority, whose identity is either part of the assertion or can be implied from the source of the assertion. The assertion may have a validity period for which it is valid, or may have an issuance time. The assertion may be signed by its issuer. Note that a privilege attribute assertion is independent of any specific authorization request while an authorization assertion is generated in response to a specific request and may rely on authorization context. See authorization assertion.

Attribute Authority (2.1, 4.1.1)
An entity that is trusted to issue attribute assertions. It may belong to the subject’s domain or to a virtual organization.

Attribute Authority Domain (4.2.1)
The domain in which a given attribute authority is recognized. Within an attribute domain, attributes are understood to have the same syntax and meaning. There may explicit shared policy with the domain as to the range of values and users about which the authority may make assertions.

Attribute Certificate IETF RFC2904, IETF RFC 3281, (3.4.1)
A structured document containing attributes used for authorization which is digitally signed using public key cryptography. IETF RFC3281 defines an X.509 attribute certificate as an ASN.1 document, that asserts an attribute about an entity that is valid within a specified period and signed by an X.509 private key.
One type of Attribute Token.

Attribute Repository (4.2.3.2)
A place to store attribute assertions. Assertions can be added to the repository by the attribute authorities and can be retrieved by a subject or by an access decision function.

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

Attribute Token (4.2.3.3)
A general term for the object which is presented as proof of right to claim an attribute. May be an attribute assertion or attribute certificate.

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 or private key).

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

Authority (2.1)
An entity asked to make decisions or create tokens which was 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 (4.1.2)
The policy which determines which authorities are accepted and how the franchises are granted.

Authorization (2.0)

Either the act of authorizing a subject to access a resource, the issuing of a token that proves such a right, or the token itself.

Authorization Agent Sequence (2.2.3)
An authorization sequence in which the subject will contact an authorization agent with a request for service, The agent makes the authorization decision, and if successful, contacts the resource to enable the service for the subject. Used in network provisioning and advanced Grid reservations.

Authorization Algorithm (4.5)
The rule(s) that is used to determine a subject's right to use a resources based all or some of the following inputs: the actions requested, the attributes of the requestor, the attributes of the resource, authorization context, environmental context and the access policy.

Authorization Architecture (3.1)
An authorization architecture consists of a set of entities and functional components that allow authorization decisions to be made and enforced based on attributes, parameters and policies that define authorization conditions.

Authorization Assertion (2.2.1, 3.4.2)
An assertion by an authorization authority that the subject (holder of the assertion) has the right to specified access on a specified resource. An authorization assertion is a response to a specific request for access. It should have a validity period specified. It may take the form of a signed certificate or a SAML authorization assertion. If it is not passed on a secured channel between the authority and the relying party, it must be signed. See attribute -privilege for contrast.

Authorization Attribute (2.5)
A named property and value associated with an entity that implicitly or explicitly defines the subjects allowed actions on some resource. There are two types of authorization attributes: descriptive attributes and privileges. A descriptive attribute is issued by an attribute authority and is independent of any resource. It consists of a named property and possibly a value. A privilege is issued by an privilege authority and grants specific rights on a resource to a subject. It consists of one or more allowed actions and a resource name.

Authorization Context (4.4)
Properties of a specific authorization request such as time, location of requester, security of the message transport and authentication of the request.

Authorization Decision (2.0.3)
The decision on what type of authorization is granted. Often this is a logical return (yes, no, undetermined) 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)
Same as access control policy.

Authorization Pull Sequence 2.2.2
An authorization sequence in which the subject makes an authenticated contact with the resource to gain access. The resource server contacts the authorization server giving it the identity of the subject. The authorization server then consults the access policy and "pulls" whatever attributes are required and possessed by the subject to make an authorization decision.

Authorization Push Sequence (2.2.1)
An authorization sequence in which the subject first contacts an authorization or attribute authority with a request to fetch attribute or authorization tokens that will allow it to access a resource. The subject then hands those tokens to the resource as a proof of its right to access the resource.

Authorization Request (3.4.2, 4.4)
A request to use a resource. The entity that wishes to use the resource may be the requestor, or may be specified as a subject of the request. In some systems, only authenticated requests from authorized entities are allowed.

Authorization Response (3.4.2, 4.5)
A response to an authorization request. The response must be securely bound to the request and when required to the responding entity. This may be accomplished by returning a signed authorization assertion, or by using a secured channel between the requestor and the authorization decision function.

Authorization Sequence RFC 2904 (2.2)
The order and content of the messages between the affected entities during an authorization decision. See push, pull and agent sequences.

Authorization Server (2.1, 4.2.1, 4.5)
The component performing the evaluation of the access policy to determine an authorization decision on behalf of the authorities.

Authorization Subject (2.1)
An entity (person or process) that is requesting, or has been granted the rights to use a resource.

Authorization System (3.1)
One particular implementation of an authorization sequence/model. It might refer to a placeholder for one implementation (e.g., 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)
A general term for a proof of a right, or reference to such a proof. May be implemented as a privilege, an authorization assertion or a capability certificate.

Certification Authorities (CA) (2.1)
A trusted entity which signs X.509 certificates that bind a public key to a distinguished name. See X.509 certificate.

Community Domain (2.3)
A set of servers, resources and users that extends beyond a single organization. Usually created to facilitate collaboration in some problem domain. Same as Virtual Organization domain.

Delegation Attribute (4.2.3)
An attribute authorizing the subject to assert some rights held by the issuer.

Domain (2.3)
A set of entities: users, severs and resources that trust the same authorities and share the same operational rules.

Enforcement of access rights (4.6)
Enforcement of access rights is the limitation of operations performed on resources on behalf of a subject to those permitted by an authoritative entity.

Environmental Authority 4.1.1
Define properties of the resource environment, such as disk usage, or machine load, or about the distributed environment such as the security of the connection or the Internet Protocol (IP) addresses of the client and server.

Holding Subjects (3.4.1)
The entity to whom an assertion applies. Must be securely bound to the assertion.

Home Domain (2.3)
The real organization to which an entity belongs.

Identity Token (2.1, 4.2.3.3)
A general term for a proof or reference to provide proof of identity. It may be implemented by an X.509 certificate, a Kerberos Ticket or a username.

Initiator ISO 10181-3
An entity (e.g. human user or computer-based entity) that attempts to access other entities.

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 policy) is typically limited to information about resource access (see Authorization Policy)

Policy Authority (2.1, 4.1.1)
This is the source of authority for a resource domain and is responsible for defining the domain's trust relationships. It also issues authorization policies with respect to resources and services offered in the domain.

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)
Specifies the criteria for issuing the appropriate authorization responses for a request to use a resource. There could be several policy statements about one resource, in which case the authorization algorithm needs to know how to combine them in making a decision.

Privilege (4.2)
A privilege grants specific rights on a resource to a subject. It consists of one or more allowed actions and a resource name. Same as privilege attribute.

Privilege Assignment (4.2.2)
The process of defining who is allowed which access rights to a resource. Privileges may be granted directly to a subject or indirectly through access policy rules.

Privilege Authority (4.2.1)

An entity that has been delegated the authority to issue privilege attributes for members of its domain with regard to resources in its own or other domains.

Privilege Management (4.1, 4.2)
The definition, acquisition, delegation and management of authorization attributes and privileges.

Proxy (4.1.2)
An entity that has all or some of the rights of the delegating entity.

Relying party
The entity that uses information such as attribute assertions, or authorization assertions to allow some actions.

Resource (2.1)
A component of a system that provides or hosts services and may enforce access to these services based on a set of rules and policies defined by entities that are authoritative for the particular resource.

Resource Authority (4.1.1)
An entity that issues policy about the use of resources.

Rights (2.1)
The permission for a subject to perform an action on a resource.

S-expressions (3.4.3.1)
Symbolic expressions (S-expressions) are a convention for representing data in text form. They are of infinite length and are structured as a branching tree, facilitating a simple isolation of sub-expressions. One can define a language using S-expressions by assigning meanings to the first element in the expression. S-expressions are used in LISP (see [McCarthy 1969]) to represent code and data and are used in SPKI to represent authorization certificates. Syntactically they consist of a list of elements where an element can also be a list.

Service (2.0)
The component that mediates access to a resource.

Service Point (2.0)
The interface that a service provides to its clients.

Service Provider RFC 2904
Same as service.

Source of Authority (SOA) (4.1.1)
The root of authority for a domain. It may be a person or group of people fulfilling a role. It may delegate parts of its authority to other authorities. It defines the trust relationships between its domain and authorities in other domains,

Subject (2.1)
An entity (e. g. a person or process) that can request, receive, own, transfer, present or delegate an electronic authorization as to exercise a certain right.

Subject Attributes (2.3, 4.2)
Attributes that are bound to subjects rather than any other component. See attribute.

Subject Domain (2.3, 4.2.1)
The home domain of the subject. Normally a real organization.

Transport Channel (4.4)
The underlying layer on which the authorization, attribute and policy requests and responses are transmitted. Of interest is what security features this layer provides.

Target ISO 10181-3
An entity, usually a resource, to which access may be attempted.

Trust (4.1)
The willingness to take actions expecting beneficial outcomes, based on assertions by other parties.

Trust Authorities (4.1.1)
The entities which are trusted to make specified assertions.

Trust Management (4.1)
Trust management defines trust authorities and specifies what they should be trusted to do.

Trust Relationships (4.1.1)
Polices which govern how entities in differing domains honor each other's authorizations. An authority may be completly trusted, e.g., any statement from the authority will be accepted as a basis for action, or there may be limited trust, in which case only statements in a specific range are accepted.

Untrusted Services (4.6.2)
Executable components that are uploaded by a user to be run at a resource site and whose content is unknown to the site administrators.

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

User Home Organization RFC 2904 (2.2)
The primary organization with which the user is associated.

Virtual Organization (2.3)
A set of users, resources and services from different home organizations that have set up common authorities and operational rules in order to share the resources for a common purpose.

Virtual Organization Domain (2.3)
A set of users, resources and services associated with a virtual organization.

Wire Format (3.4.3.4)
The format in which messages are sent across the wire between domains.

X.509 (4.2)
ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997. Defines a structured name for users and services called a distinguished name, that defines a unique name for a person by combining a common name with organizational and other components.

X.509 Certificate IETF RFC2459, (4.2.3.3)

A certificate that binds a X.509 distinguished name with a public key. When presented via a protocol that confirms that the presenter knows the private key associated with the public key in the certificate, can be used to authenticate the presenter of the certificate.

3. Expansion of Acronyms:

AAA - Authentication, Authorization, Accounting
ACL - Access Control List
ADF - Access Decision Function
AEF - Access Enforcement Point
API - Application Programming Interface
CA - Certification Authority
CAS - Community Authorization Service
GACL - Generalized Access Control List
LDAP - Light Weight Directory Protocol
NIS - Network Information Service
OGSA - Open Grid Services Architecture
PDP - Policy Decision Point
PEP - Policy Enforcement Point
PKI - Public Key Infrastructure
POSIX - Portable Operating System Interface
QoS - Quality of Service
RBAC - Role Based Access Control
SAML - Security Assertion Markup Language
SAML-P - Security Assertion Markup Language- Protocol
SOA - Source of Authority
SOAP - Simple Object Access Protocol
SPKI – Simple Public Key Infrastructure
SSL - Secure Socket Layer
VO - Virtual Organization
VOMS - Virtual Organization Membership Services
WS-Policy - Web Services Policy
WS-Security - Web Services Security
WSDL - Web Services Description Language
XACML - eXtentisible Access Control Markup Language
XML - eXchange Markup Language
XRML - eXtensible Rights Markup Language

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

Mary Thompson
Lawrence Berkeley National Laboratory
MS50B-2239
1 Cyclotron Rd.
Berkeley CA 94720
email: mrthompson@lbl.gov

Intellectual Property Statement

Full Copyright Notice

References

[McCarthy1996] McCarthy, J. et al, “LISP 1.5 Programmer’s Manual”, MIT Press, Dec. 1969

[RFC2904] Vollbrecht, J., et al, " AAA Authorization Framework", RFC 2904, August 2000.