GGF DOCUMENT SUBMISSION CHECKLIST (include as front page of submission)

	COMPLETED (X) - Date
1. Author name(s), institution(s), and contact information	X
2. Date (original and, where applicable, latest revision date)	X
3. Title, table of contents, clearly numbered sections	X
4. Security Considerations section	X
5. GGF Copyright statement inserted (See below)	X
6. GGF Intellectual Property statement inserted. (See below) **NOTE that authors should read the statement.**	X
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

GWD-I (proposed)

Von Welch, NCSA
Frank Siebenlist, Argonne National Laboratory
David Chadwick, University of Salford
Sam Meder, University of Chicago
Laura Pearlman, Information Sciences Institute

September, 2003

Use of SAML for OGSA Authorization

Status of This Memo

This document has been submitted to the Global Grid Forum OGSA Security Working Group for consideration as recommendations document in that area of OGSA authorization.

The latest version of this document can be found at:

http://www.globus.org/ogsa/Security/

Copyright Notice

Abstract

This document defines an open grid services architecture (OGSA) authorization service based on the use of the security assertion markup language (SAML) as a format for requesting and expressing authorization assertions. Defining standard formats for these messages allows for pluggability of different authorization systems using SAML.

Contents

1. Introduction

There are a number of authorization systems currently available for use on the Grid as well as in other areas of computing, such as Akenti [Akenti], CAS [CAS], PERMIS [PERMIS], VOMS [VOMS]. Some of these systems are normally used in *decision push mode* by the application [RFC2904] - they act as services and issue their authorization decisions in the form of authorization assertions that are conveyed, or pushed, to the target resource by the initiator. Others are used in *decision pull mode* by the application - they are normally linked with an application or service and act as a policy decision maker for that application, which pulls a decision from them.

On the abstract level both of these types of authorization services have similar semantics - they are given a description of the initiator (which might include the initiator's privileges), a description of an action being requested (including its argument), details about the target resource to be accessed, and any contextual information such as time of day, and they provide an authorization decision whether the action should be processed or rejected.

These authorization services can themselves act in *credential push or pull mode* [RFC3281]. In *credential push mode*, the client provides all the information necessary for a decision to be made. In *credential pull mode*, the client provides everything except the initiator's privileges, and the authorization service then pulls these privilege tokens (or credentials) from some other authority, and bases its decision on them. The client may provide a pointer to the authorization service, giving it a hint where to find the privileges, or the authorization service may be pre-configured with knowledge about where to locate them.

With the emergence of OGSA and Grid Services, it is expected that some of these systems will become OGSA authorization services as mentioned in the OGSA Security Roadmap [Roadmap]. OGSA authorization services are Grid Services providing authorization functionality over an exposed Grid Service portType. A client sends a request for an authorization decision to the authorization service and in return receives an authorization assertion or a decision. A client may be the resource itself, an agent of the resource, or an initiator or a proxy for an initiator who passes the assertion on to the resource.

This specification defines the use of SAML as a message format for requesting and expressing authorization assertions and decisions from an OGSA authorization service. This process can be single or multi-step. In single step authorization, all the information about the requested access is passed in one SAML request to the authorization service. In multi-step authorization, the initial SAML request passes information about the initiator, and subsequent SAML requests pass information about the actions and targets that the initiator wants to access.

The SAML AuthorizationDecisionQuery element is defined as the message to request an authorization assertion or decision, the DecisionStatement element is defined as the message to return a simple decision, and the AuthorizationDecisionStatement the method for expressing an authorization assertion. By defining standard message formats the goal is to allow these different authorization services to be pluggable to allow different authorization systems to be used interchangeably in OGSA services and clients.

Section 2 describes the conventions and namespaces used in this document. Section 3 contains a non-normative overview of the authorization portions of the SAML specification. Section 4 contains an non-normative description of SAML extensions defined in this document and Section 5 is a normative definition of those extensions. Section 6 is normative and defines how SAML elements should be used to form OGSA authorization assertions and requests. Section 7 contains the WSDL for the authorization service portType. Section 8 contains non-normative commentary. The specification concludes with GGF copyright and intellectual property statements, author affiliation and contact information and a glossary.

2. Conventions use in this Specification

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [RFC2119].

This specification uses namespace prefixes throughout; they are listed in Table 1. Note that the choice of any namespace prefix is arbitrary and not semantically significant.

Table 1: Namspaces used in this specification.

Prefix	Namespace
ogsa-saml	http://www.gridforum.org/namespaces/2003/06/ogsa-authz/saml/
operation	http://www.gridforum.org/namespaces/2003/06/ogsa-authz/saml/action/operation
sde-read	http://www.gridforum.org/namespaces/2003/06/ogsa-authz/saml/action/sde/read
sde-modify	http://www.gridforum.org/namespaces/2003/06/ogsa-authz/saml/action/sde/modify
wildcard	http://www.gridforum.org/namespaces/2003/06/ogsa-authz/saml/action/wildcard
saml	urn:oasis:names:tc:SAML:1.0:assertion

samlp	urn:oasis:names:tc:SAML:1.0:protocol

3. SAML Authorization Overview

The SAML specification [SAML] defines a number of elements for making assertions and queries regarding authentication, authorization decisions and attributes. It also supports extensibility by allowing applications to define their own elements. In this section we give a brief **non-normative overview** of the elements related to authorization, and the additional elements needed for Grid authorization. Readers are encouraged to review the SAML specification for more details.

3.1 SAML Authorization Model

As shown in Figure 1, SAML defines a message exchange between a policy enforcement point (PEP) and a policy decision point (PDP) consisting of an AuthorizationDecisionQuery (2) flowing from the PEP to the PDP, with an Assertion returned containing some number of AuthorizationDecisionStatements (3). We also define extensions to SAML to support exchanges in which a client can issue an AuthorizationDecisionQuery to a server, and have Assertions returned containing either an AttributeStatement or a simple AuthorizationDecision.

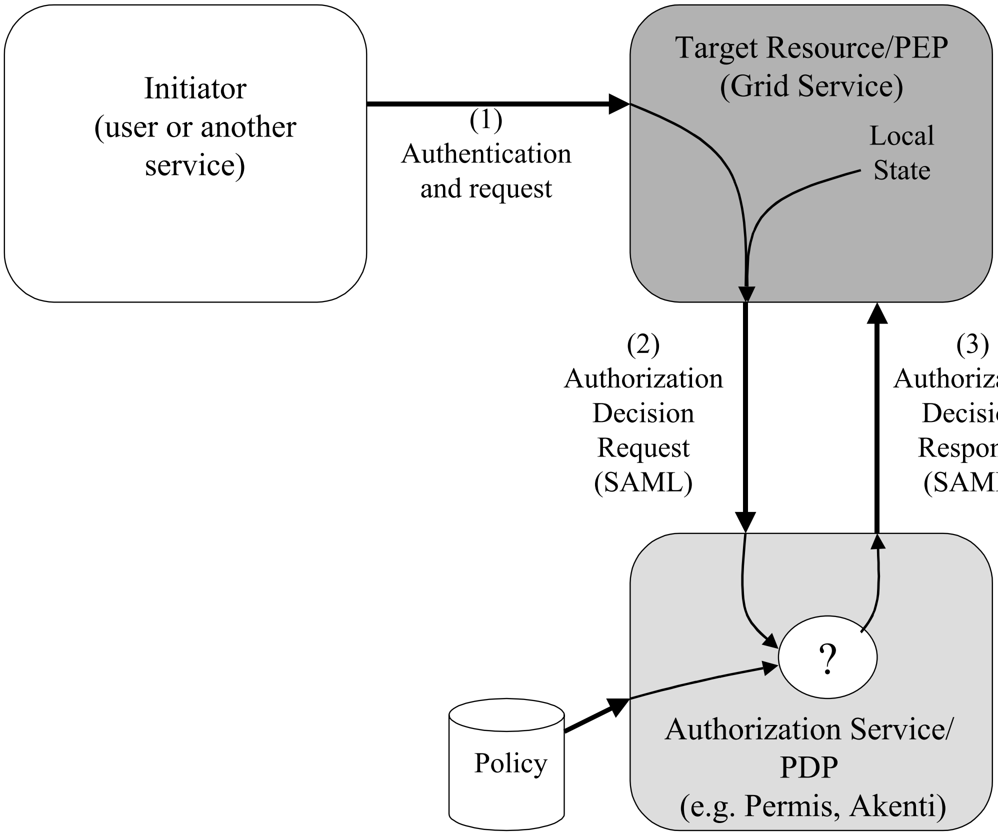
Initiator
(user or another service)
(1) Authentication and request
Target Resource/PEP
(Grid Service)
Local State
(2) Authorization Decision Request (SAML)
(3) Authorization Decision Response (SAML)
?
Policy
Authorization Service/
PDP
(e.g. Permis, Akenti)

Figure 1: SAML message flow. (1) A request arrives at the target resource. (2) The Grid Service generates and sends a SAML AuthorizationDecisionQuery to an Authorization Service. (3) The service evaluates the request against policy and returns a response encoded as a SAML Assertion.

In the following sections we describe the AuthorizationDecisionQuery and the Assertion element, and the elements that are used to compose these.

3.2 Action Element

The Action elements allows for the expression of actions that may be attempted by entities and expressed in policy. This element consists of a string and a URI defining a namespace for the action described in the string.

For example the SAML specification defines a namespace for HTTP operations that defines actions of GET, HEAD, PUT, POST.

3.3 Resource Element

The Resource element is used to identify the target on which the policy is being asserted or requested. This element is simply a URI.

3.4 Subject and NameIdentifier Elements

The Subject element contains a NameIdentifier element as well as some elements outside the scope of this document. In SAML authorization assertions, the NameIdentifer element serves to identify the initiator of the action being authorized. The NameIdentifer element contains a string to hold an identity that has two attributes:

- The NameQualifier attribute is a string expressing the security or administrative domain that defined the name (e.g. Kerberos realm, CA name).
- The Format attribute is a URI identifying the format of the name (e.g. X509 subject name).

3.5 AuthorizationDecisionStatement Element

The AuthorizationDecisionStatement element contains statements regarding authorization policy. Each of these statements contains a *Subject* element, identifying the entity whose rights are being expressed, a *Resource* element, identifying the resource(s) the rights apply to, an optional *Evidence* element holding the assertions the issuer relied upon in making its decision, any number of *Action* elements (expressing the allowed or denied operations) and the *Decision* attribute containing the authorization decision. The assertion may also have a *Conditions* element present expressing the conditions that must be fulfilled before the authorization can be permitted.

3.6 AttributeStatement Element

This element supplies a statement by the issuer that the specified subject is associated with the specified attribute(s).

3.7 Assertion Element

The Assertion element specifies the basic information that is common to all SAML assertions, and optionally it may be signed. It can contain any number of Statements, for example, AuthorizationDecisionsStatements and AttributeStatements. It is also capable of containing statements related to authentication, but for the purposes of this document we only consider Assertions containing AttributeStatements, AuthorizationDecisions and AuthorizationDecisionStatements.

3.8 Conditions Elements

Each Assertion element can also contain any number of Conditions elements. Conditions elements are specified to express policy restrictions on the assertion such as a validity time of the Assertion, however they are extendable to express arbitrary conditions on the use of the assertion. Condition elements might typically be added to assertions if the decision engine had insufficient information to be able to evaluate the policy locally.

3.9 AuthorizationDecisionQuery Element

The AuthorizationDecisionQuery element allows for the request of AttributeStatements, AuthorizationDecisionStatements and simple AuthorizationDecision responses. It contains a Subject, Resource, optional Evidence, and any number of Action elements that identify the decisions that the initiator wants to be made; as well as a RespondWith element that identifies the type of response that the client wishes to be returned.

3.10 Evidence Elements

Evidence elements allow for queries to provide information to the PDP that may be useful for its decision-making. They are used to hold the credentials of the initiator, as well as contextual and environmental information. The initiator's credentials may be either included directly in the evidence element (as AttributeStatements), or may be included indirectly via a pointer (as ReferenceStatements). This allows the PDP to support both the credential push and pull mode of operation. In responses, they also allow the PDP to express what information it used to make its decision.

Each AuthorizationDecisionStatement and AuthorizationDecisionQuery element can contain any number of Evidence elements. Each Evidence element can contain any number of Assertions elements (or references to Assertion elements) that affect the policy decision process.

3.11 ReferenceStatement Element

This element allows Authorization Decision Queries to contain a pointer to an external resource, which may contain credentials for the initiator. This is used to flag the *credential pull mode* of operation.

3.12 RespondWith Element

This element is used in queries to tell the service what type of response to provide. It is used by the client to signal if the first step of multi-step authorization is required (RespondWith an *Attribute* statement), or if a simple decision response should be returned (RespondWith a *Decision* response), or if an authorization assertion should be returned (RespondWith an *Authorization* decision statement).

4. Overview of Extensions

This section provides **non-normative** discussion of the extensions in this specification.

VW: Both of these extensions rely on the RespondWith element that is deprecated in the proposed SAML 1.1 protocol. We need to explore how we would implement these features without this element.

4.1 Simple Authorization Query Response

In the SAML authorization query protocol, a resource normally sends a query to the decision service with an enumeration of the actions being attempted by a requestor. The decision service responds with an assertion containing the set of actions that the requestor is authorized to perform.

While this functions well for situations where the resource may be interested in knowing what subset of the actions the requestor is allowed to perform, in "all or nothing" situations where the resource is only interested in knowing if the requestor can perform all the enumerated actions, it requires the resource to process the entire list to verify all the actions originally requested are listed.

This specification defines an AuthorizationDecision element which contains a reference to an AuthorizationDecisionQuery and a decision in regards to that query as a whole. Allowing an easy-to-parse decision to be rendered on the query as a whole.

VW: Maybe we just want to define a separate type of query to get a AuthorizationDecision instead of overloading AuthorizationDecisionQuery? SimpleAuthorizationDecisionQuery?

4.2 Multi-Stage Authorization

As discussed in [Authz], some Grid authorization scenarios involve the establishment of a session between a requestor and a resource in which the resource may need multiple, different, authorization decisions regarding the same requestor. To optimize processing for both the resource and the authorization decision service, it is helpful to allow the resource and decision service to establish state. The decision service can then process the request's credentials once and maintain state about the user so that subsequent queries can be responded to without reprocessing the user's credentials.

VW: I suggest we explore using stateful OGSA service instances for this instead of a context state in an attribute.

5. SAML Extensions

This section is **normative**. It defines the SAML extensions used by OGSA.

5.1 Element <AuthorizationDecision>

The <AuthorizationDecision> element specifies the decision made about the corresponding SAML AuthorisationDecisionQuery request. Its purpose is to allow the responses of "permitted” or “denied" without enumeration of the rights in the response.

It has the complex type AuthorizationDecisionType, which extends the ResponseAbstractType by adding the Decision attribute to it.

```
<element name="ogsa-saml:AuthorisationDecision" type="samlp:AuthorizationDecisionType"/>
    <complexType name="AuthorizationDecisionType">
        <complexContent>
            <extension base="samlp:ResponseAbstractType">
                <attribute name="Decision" type="saml:DecisionType" use="required"/>
           </extension>
    </complexContent>
</complexType>
```

Note that Decision is in response to the SAML request identified in the InResponseTo attribute, so this attribute MUST be present in the response.

5.2 Element <ReferenceStatement>

The <ReferenceStatement> element supplies a statement by the issuer that the designated attributes associated with the specified subject may be obtained from the referenced URI. Its purpose is to advise the PDP where it may find attributes associated with the subject, and it is used to support the *credential pull mode* of operation.

<ReferenceStatement> is of type ReferenceStatementType, which extends the SubjectStatementAbstractType with the addition of the following:

<AttributeDesignator> Element [Any number] lists the attributes that may be located at the referenced URI. If this component is absent, then it implies that all attributes can be found at the referenced URI.

<Reference> Attribute [Required] provides the URI from which the attributes may be obtained.

```
<element name="ReferenceStatement" type="saml:ReferenceStatementType"/>
    <complexType name="ReferenceStatementType">
        <complexContent>
            <extension base="saml:SubjectStatementAbstractType">
                <sequence>
                    <element ref="saml:AttributeDesignator" />
               </sequence>
               <attribute name="Reference” type=”anyURI” use="required"/>
            </extension>
    </complexContent>
</complexType>
```

6. SAML Authorization Element Usage in OGSA

This section is **normative**. It describes how SAML Authorization elements are used to meet OSGA requirements for authorization assertions and decisions as described in [Authz]. It first describes the use of the AuthorizationDecisionQuery element, which is used by entities to request authorization assertions and decisions from an authorization service. This is followed by a description of the Attribute Statement, which is used in multi-step authorization to return that the validated credentials of the initiator. Finally, the use of the Assertion element that carries the authorization assertion and decision from the authorization service to the resource is described.

6.1 AuthorizationDecisionQuery Element

The SAML AuthorizationDecisionQuery element MUST be used by a client to request an authorization service. Eight different types of authorization service are defined, namely:

- *single step authorization*, in either *credential pull or push mode*, returning either a simple AuthorizatonDecision response, or an AuthorizationDecisionStatement assertion;
- the first step of multi-step authorization in *credential push or pull mode*, returning an Attribute Statement; and
- the second step of multi-step authorization, returning either a simple AuthorizatonDecision response or an AuthorizationDecisionStatement assertion.

This element MUST includes the following elements:

- A *Subject* element containing a *NameIdentifier* element specifying the identity of the initiator.
- A *Resource* element specifying the resource (or domain of resources) to which the request to be authorized is being made.
- One or more *Action* elements specifying the action(s) being requested on the resource(s).
- A *RespondWith* element indicating the type of authorization service that is being requested.

The query MAY include the following element:

- Optionally an *Evidence* element containing one or more supporting credentials about the initiator (or pointers to them), plus any contextual information.

The following subsections describe the use of and extensions to these elements for OGSA.

6.1.1 Subject Element

This element contains the name of the initiator. The Subject and contained NameIdentifer elements are unchanged from the SAML specification. The exact use of these elements is driven by the authentication mechanism used by the client. In some scenarios, the authorization service (PDP) MAY require the initiator and client names to be the same. In other scenarios, the authorization service MAY allow trusted clients to request authorization decisions on behalf of any initiator.

The SAML specification defines how some common identity types are asserted. The Grid Security Infrastructure (GSI) is a common Grid authentication mechanism that uses X.509 based identities. The SAML specification defines a URI for X.509 subject names (#X509SubjectName) that SHOULD be used for GSI authenticated identities.

This document defines one wildcard value for the X509SubjectName of <null> i.e. an empty string, which has the special meaning of anyone (i.e. a decision about public rights is being requested). This wildcard MUST be used in order to obtain public rights.

6.1.2 Resource Element

The Resource element is defined as a URI.

In the first step of multi-step authorization, the value of this element SHOULD be ignored by the PDP, and the client MAY put any value, including null, into this element.

The following text refers to either single step authorization or the second and subsequent steps of multi-step authorization.

If the resource being referred to is a Grid service the resource element MUST contain the Grid Service Handle (GSH) of the service as described in [OGSI].

It is also possible that this element could contain a URI referring to things other than GSHs in an OGSA context. For example, a URI could be used to refer to a group of services. However such usage is determined by prior agreement between authorization services, policy makers and resources in a particular domain and is beyond the scope of this document.

This specification also defines a wildcard resource. This has two different meanings depending on whether it is in a query (request to a PDP) or a statement (response from a PDP):

- In an AuthorizationDecisionQuery, it states a desire to learn the initiator's rights on all the resource of which the authorization service is aware. Typically such a query will be used by an initiator who will cache the results and present them to resources later in a *decision push mode* of authorization.
- In an AuthorizationDecisionResponse, it states the initiator has the given privileges on all resources that accept the authorization service as authoritative. This statement may be used when the authorization service is the authority for a group of resources with identical policy.

This wildcard URI MUST be specified as follows:

http://www.gridforum.org/ogsa-authz/saml/2003/06/resource/any

6.1.3 Action Elements

The Action element describes the operation or method to be authorized. The Action element is composed of a string describing the operation and a URI specifying the namespace of the action.

In the first step of multi-step authorization, the value of this element SHOULD be ignored by the PDP, and the client MAY put any value, including null, into this element.

The following text refers to either single step authorization or the second and subsequent steps of multi-step authorization.

This specification defines the following namespaces:

http://www.gridforum.org/namespaces/2003/06/ogsa-authz/saml/action/operation

This namespace is used to define an operation invocation on the specified Resource by the specified Subject. The action string should contain the namespace and name of the operation being invoked.

http://www.gridforum.org/namespaces/2003/06/ogsa-authz/saml/action/sde/read

This namespace is used to define the reading of a ServiceDataElement. The action string should contain the QName of the Service Data element being accessed.

http://www.gridforum.org/namespaces/2003/06/ogsa-authz/saml/action/sde/modify

This namespace is used to define the modification of a ServiceDataElement. The action string should contain the QName of the Service Data element being modified.

This specification also defines a wildcard action. This action has two different meanings depending on whether it is in a query or an assertion:

- In an AuthorizationDecisionQuery, it states a desire to learn all of the initiator’s rights on the specified resource. An example of where this might be used, is by a policy enforcement point co-located with a resource, that after an intiator has set up a session, will cache the results, and do further policy processing without the authorization service.
- In an AuthorizationDecisionStatement, it states the initiator has all privileges on the resource. This will often be the case where the initiator is the policy authority for the resource in question.

This wildcard action MUST be specified as follows. The namespace URI MUST be:

```
http://www.gridforum.org/namespaces/2003/06/ogsa-authz/saml/action/wildcard
```

The Action sting must be "*", i.e., an asterisk.

6.1.4 Evidence Elements

Evidence elements are assertions used to hold, either directly or by reference, supporting credentials regarding the initiator, as well as environmental parameters.

In one step authorization the AuthorizationDecisionQuery MAY contain Evidence Elements holding environmental parameters.

In the second and subsequent steps of multi-step authorization, the AuthorizationDecisionQuery MUST contain an Evidence element holding the Attribute Assertion returned by the PDP in response to the first step of authorization and MAY contain Evidence Elements holding environmental parameters.

In one step authorization and the first step of multi-step authorization, the AuthorizationDecisionQuery MAY contain Evidence elements regarding the credentials of the initiator as follows.

In the *credential push mode* of operation this element SHOULD contain the credentials of the initiator. If the initiator does not have any credentials (for example, if default or public access rights are being requested) then there will be no evidence assertions in which the subject name is that of the initiator.[1]

In the *credential pull mode* of operation this element MAY contain a Reference Statement.

If the client wishes the PDP to operate in both credential push and pull mode, then it MAY include initiator credentials and Reference Statements in the Evidence element. If neither is present, then it is at the discretion of the PDP how to behave (e.g. it may be pre-configured with a resource from which to pull initiator credentials, or it may assume the initiator has no credentials).

This specification makes no further constraints on the use of this element for specifying credentials. It is expected that specifications for different types of supporting credentials will be developed.

6.1.5 ReferenceStatement Element

Reference statements MAY be included within Evidence elements, in order to signal the *credential pull mode* of operation to the PDP. Reference statements MAY be included instead of, or as well as, credentials in Evidence elements, and it is a local matter for the PDP to determine how to handle the presence of one, both or neither elements.

[1] Editor’s Note. Alternatively we can indicate that the initiator has no credentials, by setting this element to <AssertionIDRefence>, and the value of the string to “null”.

The value of the Reference URI is not further constrained by this specification.

6.1.6 RespondWith Element

This element MUST be used by the client to signal the type of authorization decision service being requested from the PDP. One of the following values MUST be used:

- saml:AttributeStatement – the authorization service is required to perform the first step of multi-stage authorization and return an assertion containing an saml:AttributeStatement.
- ogsa-saml:AuthorizationDecision – The authorization service is required to return a simple Authorization Decision Response to this Authorization Decision Query.
- saml:AuthorizationDecisionStatement – The authorization service is required to return an assertion containing an Authorization Decision Statement.

If single step authorization is being requested, and the client wants an AuthorizationDecisionStatement to be returned, then it MUST set the value to “saml:AuthorizationDecisionStatement”.

If single step authorization is being requested, and the client wants a simple AuthorizationDecision Response to be returned, then it MUST set the value to “ogsa-saml:AuthorizationDecision”.

If the first step of multi-step authorization is required, then the client MUST set the value to “saml:AttributeStatement”.

For second and subsequent steps in multi-step authorization, the client SHOULD set the value to either “ogsa-saml:AuthorizationDecision” or “saml:AuthorizationDecisionStatement” dependent upon the type of response that is required.

If a client follows an AuthorizationDecisionQuery with RespondWith set to “Attribute” with another AuthorizationDecisionQuery with RespondWith set to “saml:AttributeStatement” and the subject elements are identical in the two queries, then the Attribute Statement returned on first request is effectively superceded by the Attribute Statement returned in the subsequent request.

6.2 Assertion Element

The SAML Assertion element is used by one entity to assert the capabilities of another. While an Assertion element can contain a variety of SAML statements, for the purposes of this document we consider only AuthorizationDecisionStatements and AttributeStatements. The former are returned in one-step authorization or the second and subsequent steps of multi-step authorization, whilst the latter are returned in the first step of multi-step authorization.

When returned by an authorization service to an entity, the Assertion element will be enveloped in a SAML Response element as described in the SAML specification.

The Assertion element includes the following elements:

- An optional *Conditions* element specifying the conditions for use of the assertion.
- An optional *Advice* element specifying advice for use of the element.
- Any number of *AuthorizationDecisionsStatements* or *AttributeStatements* specifying capabilities.
- An optional *Signature* element allowing the Assertion to be verified.

The following subsections describe the use and extensions to these elements for OGSA.

6.2.1 Conditions Element

Implementations are advised to be conservative in their use of this element and only include it when they are confident it will be understood.

The Conditions element contains optional time constraints and any number of Condition elements (note difference in plurality between element names) on the returned assertion. Condition elements serve as an abstract element for extension, and should be used to express the policy conditions on operands and context/environment that the authorization service was unable to evaluate due to insufficient information being provided by the client. It is envisioned that future specification will be able to extend the Condition element to return fine-grained policies for parameters on operation invocation and service data access, using for example elements of XACML.

6.2.2 Advice Element

This specification recommends against the use of the Advice element. Implementations SHOULD NOT use this element and MAY only include it when they are confident it will be understood.

6.2.3 AuthorizationDecisionStatement Element

The AuthorizationDecisionStatement element contains the same elements as the AuthorizationDecisionQuery, and also includes a Decision attribute.

The Decision attribute can take the value of Permit, Deny or Indeterminate. If a value of Indeterminate is returned, then the encapsulating assertion MUST also have a *Conditions* element present expressing the conditions that MUST be fulfilled before the authorization can be permitted[2].

Comment from Mary Thompson: Conditions need to be associated with specific actions not just with an Authorization Decision Statement (ADS) as section 6.2.3 seems to imply. Actually going back through the SAML schema, a SAML response can contain 0 to unbounded assertions, and the assertion contains the conditions and the ADS which in turn contains the actions and permission.

So if in section 6.2 you point out that the SAML response element may contain one or more assertions, then in 6.2.3 you can mention that if some actions have different conditions than others, they should be returned in different assertions, and not just different ADS's. If they have the same (or all null conditions) but different Decisions they can be in the same assertion but different ADS's.

6.2.4 AttributeStatement Element

The AttributeStatement element MUST be sent in a reply to an AuthorizationDecisionQuery in which the RespondWith element value was set to “Attribute” i.e. to the first step of multi-step authorization.

The returned Attribute Statement SHOULD contain a PDP encoded cookie that is associated with the initiator (subject element of the AuthorizationDecisionQuery). For example, when RBAC is being used, the attribute statement could contain the list of validated roles of the initiator. Whether the cookie is opaque or understandable by the client is currently out of the scope of this document. However, the returned attribute statement MUST be usable multiple times by the client in subsequent AuthorizationDecisionQueries concerning the same initiator.

When the assertion encapsulating the Attribute Statement is returned across an insecure network, it SHOULD be signed by the PDP.

The client SHOULD use the returned attribute assertion and insert it into the Evidence element of all subsequent AuthorizationDecisionQueries sent to the same PDP for the same subject/initiator. In subsequent queries the RespondWith element SHOULD be set to “Decision” or “Authorization”.

[2] We have to decide on the best way of returning a conditional response. There are a couple of possibilities. I) return Permit with Conditions (but the conditions have to be evaluated to true before the permit is valid) II) return Indeterminate with Conditions (and the decision then depends upon the evaluation of the conditions). II) has been chosen above.

6.2.5 Signature Element

This specification places no constrains on the Signature elements. Implementations SHOULD sign assertions when they do not have an authenticated connection to the evaluator of the assertion.

7. SAML Authorization Service PortType

XXX To be defined

8. Commentary

This section contains **non-normative** commentary.

8.1 Proposed SAML 1.1 specification

The OASIS Security Services Technical Committee (SSTC) [SSTC] has ratified a new version, version 1.1, of SAML. That document contains changes which affect the contents of this document.

A document describing differences can be found at:

http://www.oasis-open.org/committees/download.php/2247/sstc-saml-diff-1.1-draft-01.doc

The new SAML 1.1 specification contains the following changes, which need to be integrated into this document:

1. The URI to identify X.509 subject names is changed. This specification recommends this URI for GSI subject identities.
2. The RepondWith element is deprecated. This specification uses this element to request an attribute for multi-step authorization and needs to find a different way to accomplish this.

9. Security Considerations

This specification defines an authorization service based on the SAML specification for OGSA and is completely about security. Implementers of this specification need to be aware that errors in implementation could lead to denial of service or improper granting of service to unauthorized users.

In particular, implementations should verify versions of assertions they are relying on and discount any version their software is not familiar with.

Author Information

Von Welch
National Center for Supercomputing Applications
vwelch@ncsa.uiuc.edu

Frank Siebenlist
Argonne National Laboratory
franks@mcs.anl.gov

Sam Meder
University of Chicago
meder@mcs.anl.gov

Laura Pearlman
Information Sciences Institute
University of Southern California
laura@isi.edu

David Chadwick
Information Systems Institute
University of Salford
d.w.Chadwick@salford.ac.uk

Glossary

The following terms are abbreviations are used in this document.

ACI – Access Control Information (from ISO 10181-3). Any information used for access control purposes, including contextual information.

ADF – Access control Decision Function (from ISO 10181-3). A specialized function that makes access control decisions by applying access control policy rules to an access request, ADI (of initiators, targets, access requests, or that retained from prior decisions), and the context in which the access request is made.

ADI – Access control Decision Information (from ISO 10181-3). The portion (possibly all) of the ACI made available to the ADF in making a particular access control decision.

AEF – Access control Enforcement Function (from ISO 10181-3). A specialized function that is part of the access path between an initiator and a target on each access request and enforces the decision made by the ADF.

Client – the entity making a decision request to the ADF (it could be the target, the initiator, or a proxy acting on behalf of the initiator)

Contextual information – Information about or derived from the context in which an access request is made (e.g. time of day).

Environmental parameters – same as contextual information.

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

PDP – same as ADF

PEP – same as AEF

Privilege – An attribute or property assigned to an entity by an authority

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

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

References

[Akenti] Thompson, M., et al., "Certificate-based Access Control for Widely Distributed Resources," in Proc. 8th Usenix Security Symposium. 1999.

[Authz] Welch, V., et al, OGSA Authorization Requirments, June, 2003.

[CAS] Pearlman, L., V. Welch, I. Foster, C. Kesselman, S. Tuecke, "A Community Authorization Service for Group Collaboration," Proceedings of the IEEE 3rd International Workshop on Policies for Distributed Systems and Networks, 2002.

[OGSI] Foster, I., C. Kesselman, J. Nick, S. Tuecke, "The Physiology of the Grid: An Open Grid Services Architecture for Distributed Systems Integration," Open Grid Service Infrastructure WG, Global Grid Forum, June 22, 2002.

[PERMIS] Chadwick, D.W., O.Otenko, " The PERMIS X.509 Role Based Privilege Management Infrastructure", Proceedings of 7th ACM Symoisium on Access Control Models and Technologies (SACMAT 2002).

[Roadmap] Siebenlist, F., et al, "OGSA Security Roadmap," OGSA Security WG, Global Grid Forum, July, 2002.

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

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997.

[RFC3281] Farrell, S., Housley, R. “An Internet Attribute Certificate Profile for Authorization”, RFC 3281, May 2002.

[SSTC] OASIS Security Services Technical Committee, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security, June, 2003.

[VOMS] "VOMS Architecture v1.1," http://grid-auth.infn.it/docs/VOMS-v1_1.pdf, February 2003.

ChangeLog

Version 02, September 2003:

- Minor editorial corrections from Mary Thompson.
- Comment in 6.2.3 from Mary Thompson.
- 8.1: SAML 1.1 is now an official OASIS standard.

Version 01, June 2003: Initial Revision