Geopriv
Internet-Draft
Expires: August 17, 2005

C. Guenther
Siemens

February 13, 2005

SAML in Authorization Policies
draft-guenther-saml-policy-00.txt

Status of this Memo

Copyright Notice

Abstract

Rules of an authorization policy prescribe under which conditions an entity or subject has which permissions. Existing policies support identity-based authorization by matching the authenticated identity of the entity requesting access to a resource with the available policies. This document is about formulating policy rules that express conditions with respect to SAML assertions, thereby supporting non-identity-based authorization and anonymity.

Table of Contents

1. Introduction

The Security Assertion Markup Language, see [SAML], is an XML sublanguage for exchanging security information. It is suitable for expressing assertions concerning previously performed authentication procedures and authorization decisions. For example, a SAML assertion can be used by the assertion issuer to assure that the assertion subject (e.g., a person, a network entity, ...) has been authenticated by means of a specific authentication method M. A recipient of such an assertion - if it has trust in the assertion issuer and the integrity of the assertion - can then base its authorization decisions on this assertion.

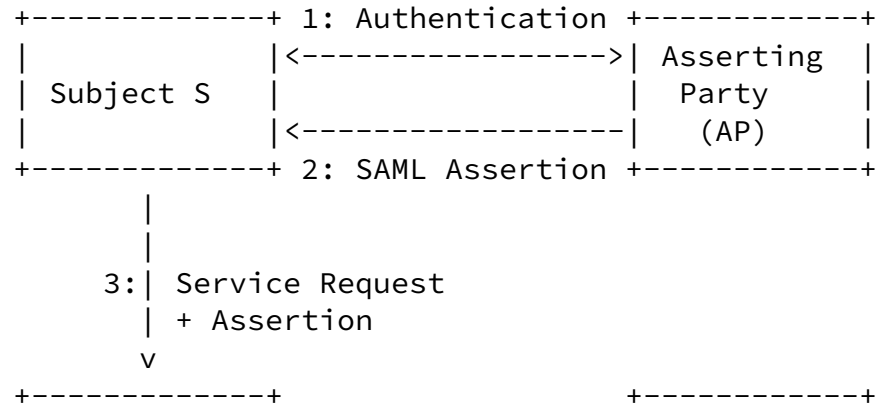
This document is about defining an extension to the Common Policy markup language, see [I-D.ietf-geopriv-common-policy], that allows to express conditions with respect to statements contained in SAML assertions. It shall be possible to express authorization policy rules of the following fashion: If the SAML assertion has been issued by the assertion issuer A and if the assertion assures that the assertion subject S has been authenticated by means of the authenticated method M, then S is permitted to ... .

2. Terminology

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 [RFC2119].

3. Basic Scenario

Figure 1 depicts a basic scenario in the scope of this document: a Subject S wishes to have access to a certain resource (e.g., location information of a particular entity). After a successful authentication protocol execution between S and the Asserting Party (AP), see step 1, the AP issues a SAML assertion (step 2), which asserts that S has been authenticated by AP using method M and is associated with a certain set of attributes.



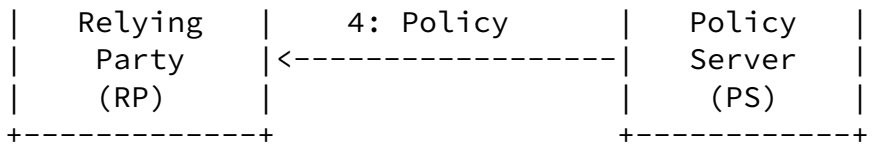


Figure 1: Basic Scenario

After receipt of the assertion, the Relying Party (RP) can base its resource access authorization decision on this assertion. The authorization policy governing access to the requested resource is stored at the Policy Server (PS). Thanks to the language elements introduced in this document, this policy can contain rules whose conditions parts express properties that the SAML assertion must meet in order to make the rule match.

4. SAML Conditions Example

This document extends the Common Policy markup language by adding new elements to the <condition> substitution group defined in the schema of the Common Policy markup language, see [I-D.ietf-geopriv-common-policy]. This paragraph provides a basic example of an XML document valid with respect to the XML schema defined in Section 5.

```
<?xml version="1.0" encoding="UTF-8"?>
<ruleset
  xmlns="urn:ietf:params:xml:ns:common-policy"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:samlc="urn:ietf:params:xml:ns:saml-cond"
```

```
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation=
    "urn:ietf:params:xml:ns:common-policy cp.xsd
     urn:ietf:params:xml:ns:saml-cond sc.xsd
     urn:oasis:names:tc:SAML:2.0:assertion
       sstc-saml-schema-assertion-2.0.xsd ">

  <rule id="Hz90op54I">

    <conditions>

      <samlc:samlcondition>
        <saml:Issuer>https://www.idp.com/</saml:Issuer>

        <samlc:authnstatement>
          <samlc:authncontextclassref>
  urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
          </samlc:authncontextclassref>
        </samlc:authnstatement>

      </samlc:samlcondition>

      <validity>
        <from>2005-03-06T17:00:00-05:00</from>
        <to>2005-03-11T19:00:00-05:00</to>
      </validity>

    </conditions>

    <actions></actions>

  </rule>
```



```
</ruleset>
```

The rule set in this example consists of one rule only. The <conditions> part of the rule consists of a <validity> condition (defined by the Common Policy schema) and a <samlcondition> condition which is defined by this document in Section 5. As there is no <Subject> subelement of <samlcondition>, this rule matches for each Subject identified in a SAML authentication assertion issued by

idp.com that asserts that the Subject has been authenticated through the presentation of a password over a protected session (e.g., protected by SSL or IPSec).

5. XML Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="urn:ietf:params:xml:ns:saml-cond"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:cp="urn:ietf:params:xml:ns:common-policy"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified">

  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:assertion"
    schemaLocation="sstc-saml-schema-assertion-2.0.xsd"/>
  <xs:import namespace="urn:ietf:params:xml:ns:common-policy"
    schemaLocation="cp.xsd"/>

  <xs:element name="samlcondition" substitutionGroup="cp:condition">
    <xs:complexType>
     <xs:sequence>

        <xs:element ref="saml:Issuer" minOccurs="0"/>
        <xs:element ref="saml:Subject" minOccurs="0"/>

        <xs:element name="authnstatement"
           minOccurs="0" maxOccurs="unbounded">
           <xs:complexType>
             <xs:sequence>
               <xs:element name="authncontextclassref" type="anyURI"
                  minOccurs="0" maxOccurs="unbounded"/>
             </xs:sequence>
           </xs:compleyType>
        </xs:element>

      </xs:sequence>
    </xs:complexType>
  </xs:element>

</xs:schema>
```

6. Security Considerations

[tbd]

7. IANA Considerations

[tbd]

8. Open Issues

1) There are not only authentication assertions in SAML, but also authorization decision and attribute assertions. Inspect the usability of these types of SAML assertions in the scope of this document.

2) Modify and enhance the XML schema in accordance to 1). Possibly, it could be more appropriate to directly adopt XML element and type definitions as given in the SAML assertion schema instead of defining new ones.

3) It could be useful to let the <samlcondition> element represent an XML schema that specizializes the SAML assertion schema with respect to the target of the authorization policy. Example: Instaed of listing all permitted authentication context class references in <authncontextclassref>, you could write down a target-specific SAML assertion schema with an <AuthnContextClassRef> element whose definition is completely identical to the SAML definition of <AuthnContextClassRef>, except for the fact that only certain URIs are permitted as values to make the SAML assertion valid with respect to this specialized assertion schema.

4) Security considerations.

5) IANA considerations.

9. Normative References

[I-D.ietf-geopriv-common-policy]
Schulzrinne, H., Morris, J., Tschofenig, H., Polk, J. and J. Rosenberg, "A Document Format for Expressing Privacy

Preferences", Internet-Draft draft-ietf-common-policy-03, October 2004.

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

[SAML] OASIS, "Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0", OASIS Committee Draft sstc-saml-core-2.0-cd-04.pdf, January 2005.

Author's Address

Christian Guenther
Siemens
Otto-Hahn-Ring 6
Munich, Bayern 81739
Germany

Email: christian.guenther@siemens.com

Intellectual Property Statement

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.