SAML Protocols -- draft-sstc-protocols-00

Core Assertions & Protocols Subgroup,

OASIS Security Services Technical Committee (SSTC)
10-Apr-2001

Tim Moses

The basic data objects of the SAML protocol model are "Assertions" and "References" (to Assertions). Assertions are of two different types: "authentication" and "attribute". The resulting four data objects, in their current versions, are represented in the SAML namespace. Syntax definitions for the various types of assertion can be found elsewhere.

(Note: the decision assertion is eliminated, by allowing the PEP to request an attribute assertion (or reference thereto) that affirms the question to be decided (e.g. such-and-such a Principal occupies such-and-such a role, or such-and-such a Principal is permitted to perform such-and-such an action on such-and-such an object. If the PDP returns the requested assertion (or reference thereto), without modification, it has effectively answered "Yes" to the question).

The SAML protocol specification defines a Request/Response pair of messages by which the Requestor requests that the Responder issue an assertion of a specified type. If a suitable assertion already exists, then that assertion may be returned in response to the request, without the responder having to create a new one. Even for the case where the PEP requests that the PDP return a specified list of attributes for an identified Principal, the response is treated as an assertion whose authenticity is vouched for by the PDP.

This scope does not include the request by a Principal to a PEP for access to a resource. This aspect will be addressed directly by the "Bindings" working group.

The following entities in the protocol model may adopt the role of Requestor in the exchange: Principal, PEP, PDP and Authority. The following entities in the protocol model may adopt the role of Responder in the exchange: Authority and PDP. Table 1 shows typical applications of the messages.

Requestor	Responder	Typical application
Principal	Authority	The Authority returns an authentication or attribute assertion (or reference thereto) with the Principal as subject
Authority	PDP	The PDP returns an authentication or attribute assertion (or reference thereto) with a Principal designated by the Authority as subject
PEP	PDP	The PDP returns an attribute assertion (or reference thereto) with a Principal designated by the PEP as subject
PDP	Authority	The Authority returns an authentication or attribute assertion with a Principal designated by the PDP as subject

Table 1 - Typical applications of the request/response messages

The request is in the form of a "prototype" of the required assertion. Each attribute of the required assertion is represented in the prototype by a "type"/"value" pair. The requestor may omit the "value" field, if it does not know, or care, what value should be assigned to the corresponding element in the resulting assertion. The responder may modify the requested values. It may also omit requested elements and it may add additional elements. These actions are reflected in the "status" element of the response.

In addition to the prototype assertion, the Requestor may supply some or all of the information required by the Responder to prepare the requested assertion. The additional information may take the form of:

- Assertions of any type,
- References to assertions of any type, and
- Information about the Principal (such as its posited name and authenticator).

(Note: XML schemas are used here to define the contents of the request and response messages. However, it is not the intention that messages conformant with these schemas will actually form the messages exchanged between parties in the SAML model. The precise contents of messages will depend on the transport protocols to which they are bound, and it is the task of the "Bindings" working group to define the precise message contents for each transport protocol. The schemas defined here serve merely as guidance to the "Bindings" working group.)

There are two basic message types, the Request message and the corresponding Response message. The Request message contains the following fields.

```
<element name = "RequestIdentifier" type = "string"/>
<element name = "PrototypeAssertionsList">
        <element name = "PrototypeAssertion" minOccurs = "0" maxOccurs = "unbounded" >
                <complexType>
                        <sequence>
                                <element name = "FieldType" type = "string"/>
                                <element name = "FieldValue" type = " … " minOccurs = "0"/>
                        </sequence>
                </complexType>
        </element>
</element>
<element name = "SupportingInformation" type = "SupportingInformation"/>
</element>
```

The FieldType string is the name of the element requested to be present in the assertion returned by the responder.
The FieldValue value is the value requested for that element.

(Note: an alternative way to handle this is to include a conformant assertion whose field values are set to some special value that indicates they are to be completed.)

```
<element name = "SupportingInformation">
```

```
        <complexType>
                <sequence>
                        <element name = "Reference" type = "string" minOccurs = "0" maxOccurs = "1" />
                        <element name = "Assertion" type = "SamlAssertion" minOccurs = "0" maxOccurs = "unbounded"/>
                        <element name = "Principal" type = "Principal" minOccurs = "0" maxOccurs = "1"/>
                </sequence>
        </complexType>
</element>

<element name = "Principal">
        <complexType>
                <sequence>
                        <element name = "Name" type = "Name" minOccurs = "0" maxOccurs = "1" />
                        <element name = "Authenticator" type = "Authenticator" minOccurs = "0" maxOccurs = "unbounded"/>
                </sequence>
        </complexType>
</element>
```

The "Authenticator" element is yet to be defined. However, it must be capable of accommodating a salted password digest, a cryptographic challenge/response pair or a document/signature pair.

The Response message contains the following fields.

```
<element name = "RequestIdentifier" type = "string"/>
<element name = "AssertionsList">
        <element name = "Assertion" minOccurs = "0" maxOccurs = "unbounded">
                <complexType>
                        <sequence>
                                <element name = "Assertion" type = "SamlAssertion"/>
                                <element name = "Status" type = "Status"/>
```

```
                        </sequence>
                    </complexType>
                </element>
            </element>
        </element>
```