## 3.7 Single Logout Protocol

The single logout protocol provides a message exchange protocol by which all sessions provided by a particular session authority are near-simultaneously terminated. The single logout protocol is used either when a principal logs out at a session participant or when the principal logs out directly at the session authority. This protocol may also be used to log out a principal due to a timeout. The reason for the logout event can be indicated through the Reason attribute.

The principal may have established authenticated sessions with both the session authority and individual session participants, based on assertions containing authentication statements supplied by the session authority.

When the principal invokes the single logout process at a session participant, the session participant MUST send a <LogoutRequest> message to the session authority that provided the assertion containing the authentication statement related to that session at the session participant.

When either the principal invokes a logout at the session authority, or a session participant sends a logout request to the session authority specifying that principal, the session authority SHOULD send a <LogoutRequest> message to each session participant to which it provided assertions containing authentication statements under its current session with the principal, with the exception of the session participant that sent the <LogoutRequest> message to the session authority. It SHOULD attempt to contact as many of these participants as it can using this protocol, terminate its own session with the principal, and finally return a <LogoutResponse> message to the requesting session participant, if any.

## 3.7.1 Element <LogoutRequest>

A session participant or session authority sends a <LogoutRequest> message to indicate that a session has been terminated.

The <LogoutRequest> message SHOULD be signed or otherwise authenticated and integrity protected by the protocol binding used to deliver the message.

This message has the complex type LogoutRequestType, which extends RequestAbstractType and adds the following elements and attributes:

NotOnOrAfter [Optional]

The time at which the request expires, after which the recipient may discard the message. The time value is encoded in UTC, as described in Section 1.3.3. [E92] As noted in section 1.3.3, relying parties SHOULD allow for reasonable clock skew in the interpretation of both values.

Reason [Optional]

An indication of the reason for the logout, in the form of a URI reference. [E10] The Reason attribute is specified as a string in the schema. This specification further restricts the schema by requiring that the Reason attribute MUST be in the form of a URI reference.

<saml:BaseID> or <saml:NameID> or <saml:EncryptedID> [Required]

The identifier and associated attributes (in plaintext or encrypted form) that specify the principal as currently recognized by the identity and service providers prior to this request. (For more information on this element, see Section 2.2.)

<SessionIndex> [Optional] [E38]

The index of the session between the principal identified by the <saml:BaseID>, <saml:NameID>, or <saml:EncryptedID> element, and the session authority. This must correlate to the SessionIndex attribute, if any, in the <saml:AuthnStatement> of the assertion used to establish the session that is being terminated.

The following schema fragment defines the <LogoutRequest> element and associated LogoutRequestType complex type:

<element name="LogoutRequest" type="samlp:LogoutRequestType"/>

<complexType name="LogoutRequestType">

<complexContent>

<extension base="samlp:RequestAbstractType">

<sequence>

<choice>

<element ref="saml:BaseID"/>

<element ref="saml:NameID"/>

<element ref="saml:EncryptedID"/>

</choice>

<element ref="samlp:SessionIndex" minOccurs="0" maxOccurs="unbounded"/>

</sequence>

<attribute name="Reason" type="string" use="optional"/>

<attribute name="NotOnOrAfter" type="dateTime" use="optional"/>

</extension>

</complexContent>

</complexType>

<element name="SessionIndex" type="string"/>

</element>

## 3.7.2 Element <LogoutResponse>

The recipient of a <LogoutRequest> message MUST respond with a <LogoutResponse> message, of type StatusResponseType, with no additional content specified.

The <LogoutResponse> message SHOULD be signed or otherwise authenticated and integrity protected by the protocol binding used to deliver the message.

The following schema fragment defines the <LogoutResponse> element:

<element name="LogoutResponse" type="samlp:StatusResponseType"/>

## 3.7.3 Processing Rules

The message sender MAY use the Reason attribute to indicate the reason for sending the <LogoutRequest>. The following values are defined by this specification for use by all message senders; other values MAY be agreed on between participants:

urn:oasis:names:tc:SAML:2.0:logout:user

Specifies that the message is being sent because the principal wishes to terminate the indicated session.

urn:oasis:names:tc:SAML:2.0:logout:admin

Specifies that the message is being sent because an administrator wishes to terminate the indicated session for that principal.

All other processing rules associated with the underlying request and response messages MUST be observed.

Additional processing rules are provided in the following sections.

## 3.7.3.1 Session Participant Rules

When a session participant receives a <LogoutRequest> message, the session participant MUST authenticate the message. If the sender is the authority that provided an assertion containing an authentication statement linked to the principal's current session, the session participant MUST invalidate the principal's session(s) referred to by the <saml:BaseID>, <saml:NameID>, or <saml:EncryptedID> element, and any <SessionIndex> elements supplied in the message. If no <SessionIndex> elements are supplied, then all sessions associated with the principal MUST be invalidated.

* The session participant MUST apply the logout request message to any assertion that meets the following conditions, even if the assertion arrives after the logout request:
* The subject of the assertion strongly matches the <saml:BaseID>, <saml:NameID>, or <saml:EncryptedID> element in the <LogoutRequest>, as defined in Section 3.3.4.
* The SessionIndex attribute of one of the assertion's authentication statements matches one of the <SessionIndex> elements specified in the logout request, or the logout request contains no <SessionIndex> elements.
* The assertion would otherwise be valid, based on the time conditions specified in the assertion itself (in particular, the value of any specified NotOnOrAfter attributes in conditions or subject confirmation data).
* The logout request has not yet expired (determined by examining the NotOnOrAfter attribute on the message).

**Note**: This rule is intended to prevent a situation in which a session participant receives a logout request targeted at a single, or multiple, assertion(s) (as identified by the <SessionIndex> element(s)) before it receives the actual – and possibly still valid - assertion(s) targeted by the logout request. It should honor the logout request until the logout request itself may be discarded (the NotOnOrAfter value on the request has been exceeded) or the assertion targeted by the logout request has been received and has been handled appropriately.

## 3.7.3.2 Session Authority Rules

When a session authority receives a <LogoutRequest> message, the session authority MUST authenticate the sender. If the sender is a session participant to which the session authority provided an assertion containing an authentication statement for the current session, then the session authority SHOULD do the following in the specified order:

* Send a <LogoutRequest> message to any session authority on behalf of whom the session authority proxied the principal's authentication, unless the second authority is the originator of the <LogoutRequest>.
* Send a <LogoutRequest> message to each session participant for which the session authority provided assertions in the current session, other than the originator of a current <LogoutRequest>.
* Terminate the principal's current session as specified by the <saml:BaseID>, <saml:NameID>, or <saml:EncryptedID> element, and any <SessionIndex> elements present in the logout request message.

If the session authority successfully terminates the principal's session with respect to itself, then it MUST respond to the original requester, if any, with a <LogoutResponse> message containing a top-level status code of urn:oasis:names:tc:SAML:2.0:status:Success. If it cannot do so, then it MUST respond with a <LogoutResponse> message containing a top-level status code indicating the error. Thus, the top-level status indicates the state of the logout operation only with respect to the session authority itself.

The session authority SHOULD attempt to contact each session participant using any applicable/usable protocol binding, even if one or more of these attempts fails or cannot be attempted (for example because the original request takes place using a protocol binding that does not enable the logout to be propagated to all participants).

In the event that not all session participants successfully respond to these <LogoutRequest> messages (or if not all participants can be contacted), then the session authority MUST include in its <LogoutResponse> message a second-level status code of urn:oasis:names:tc:SAML:2.0:status:PartialLogout to indicate that not all other session participants successfully responded with confirmation of the logout.

Note that a session authority MAY initiate a logout for reasons other than having received a <LogoutRequest> from a session participant – these include, but are not limited to:

* If some timeout period was agreed out-of-band with an individual session participant, the session authority MAY send a <LogoutRequest> to that individual participant alone.
* An agreed global timeout period has been exceeded.
* The principal or some other trusted entity has requested logout of the principal directly at the session authority.
* The session authority has determined that the principal's credentials may have been compromised.

When constructing a logout request message, the session authority MUST set the value of the NotOnOrAfter attribute of the message to a time value, indicating an expiration time for the message, after which the logout request may be discarded by the recipient. This value SHOULD be set to a time value equal to or greater than the value of any NotOnOrAfter attribute specified in the assertion most recently issued as part of the targeted session (as indicated by the SessionIndex attribute on the logout request).

In addition to the values specified in Section [E0] 3.7.3 for the Reason attribute, the following values are also available for use by the session authority only:

urn:oasis:names:tc:SAML:2.0:logout:global-timeout

Specifies that the message is being sent because of the global session timeout interval period being exceeded.

urn:oasis:names:tc:SAML:2.0:logout:sp-timeout

Specifies that the message is being sent because a timeout interval period agreed between a participant and the session authority has been exceeded.