

WSDL and SOAP bindings for WSPL

Draft 1, 11 June 2003

1. WSDL 1.1

1.1 Introduction

As a precursor to invoking a wsdl/operation of a wsdl/port, certain consumer configuration steps are likely to be required, and these configuration steps are likely to be associated with the corresponding wsdl/portType, rather than an individual wsdl/operation. Locating, retrieving, validating and compiling policy are appropriate functions to perform as one of these configuration steps.

Different aspects of policy may be most applicable to different objects within a wsdl/portType definition. For instance, privacy policy may apply to a wsdl/message definition, regardless of which wsdl/operation uses the wsdl/message. Crypto-security policy, on the other hand, may apply to a wsdl/message definition, differently, according to which wsdl/operation uses the wsdl/message. And, trust policy may apply to the wsdl/portType, independent of which wsdl/operation or wsdl/message is used.

1.2 Attachment

For the reasons stated in the Introduction, top-level xacml/PolicySet elements SHALL be targeted only at wsdl/portType elements. However, it MUST be possible to associate a policy statement with any of the objects (wsdl/portType, wsdl/operation and wsdl/message) either alone or in combination. For this reason, policy statements MUST be capable of differentiating between the various wsdl/operation and wsdl/message definitions of the wsdl/portType element at which they are targeted.

The WSDL schema requires that wsdl/portType, wsdl/operation and wsdl/message elements have a name attribute of type NCName. This attribute can be used to associate policies with particular wsdl/portType, wsdl/operation, wsdl/message elements or combinations thereof. URLs are a form of NCName.

1.3 Structure

Conformant xacml/PolicySet elements SHALL be structured as follows:

The top-level element SHALL be an xacml/PolicySet element whose xacml/PolicySet/Target/Resources element identifies the wsdl/portType to which it is applicable, by means of the wsdl/portType@name attribute.

Policies that apply to the wsdl/portType, regardless of wsdl/operation or wsdl/message SHALL be contained in xacml/Policy elements immediately subordinate to the top-level xacml/PolicySet element.

The next level SHALL contain xacml/PolicySet elements whose xacml/PolicySet/Target/Actions element SHALL identify the wsdl/operation, and whose xacml/PolicySet/Target/Resources element SHALL identify the wsdl/message definitions to which they are applicable. Only wsdl/message definitions of the "input" type SHALL be identified.

Policies that apply to some combination of wsdl/portType, wsdl/operation and wsdl/message SHALL be contained in xacml/Policy elements within this xacml/PolicySet element.

The xacml/Policy/Target/Resources element SHALL identify the **aspect** of policy to which it applies.

1.4 Integrity/authenticity protection

If the wsdl/definitions element is integrity-protected, then the xacml/PolicySet elements SHOULD be included within the integrity-protection of that element.

Where it is not possible to do this, either because the wsdl/definitions element is not integrity-protected, or for other reasons, xacml/PolicySet elements SHALL be enclosed in a saml/Assertion element wrapper. This allows supporting information, such as the saml/Assertion@Issuer attribute to be attached. The saml/Assertion element SHALL be integrity-protected.

The policy-user SHALL ignore the xacml/PolicySet@PolicySetId attribute.

The wsdl/portType to which a policy applies SHALL be identified in the policy's xacml/PolicySet/Target/Resources element, by means of the wsdl/portType@name attribute. The policy-user SHALL confirm that it has located the correct policy by examining the policy's xacml/PolicySet/Target/Resources element. Furthermore, if they are present, the policy-user SHALL confirm that the policy is current, by examining the saml/Assertion/Conditions@NotBefore and saml/Assertion/Conditions@NotOnOrAfter attributes.

The wsdl/portType@name attribute SHALL contain a URL. In the case where a policy is wrapped in a saml/Assertion, the host and domain parts of the wsdl/portType@name attribute value SHALL be identical to the saml/Assertion@Issuer attribute value. The saml/Assertion@Issuer attribute value SHALL be identical to the CN attribute value in the subject field of the certificate that validates the saml/Assertion element, whether integrity protection is provided by SSL or XML Digital Signature.

2. SOAP

2.1 Introduction

In the case of a request-response-operation, consumer policies for the response message MAY be conveyed in a SOAP header of the corresponding request message. The names assigned to objects by the consumer are not guaranteed to match those assigned by the provider to the equivalent objects. Therefore, the names assigned by the **provider** SHALL be used to associate consumer policy with wsdl objects. This means that response policies MUST be tailored to the particular provider, and the consumer may require a different policy for each provider of the same service.

In the case of the solicit-response-operation and the notification-operation, the WSDL technique, described above, SHALL be used to disseminate consumer policy.

2.2 Structure

Conformant xacml/PolicySet elements SHALL be structured as described in Section 1.3, above. Only wsdl/message definitions of the "output" or "fault" types SHALL be targeted by policies.

2.3 Integrity/authenticity protection

If the soap/header element is integrity-protected, then the xacml/PolicySet elements SHOULD be included within the integrity-protection of that element.

Where it is not possible to do this, either because the soap/header element is not integrity-protected, or for other reasons, xacml/PolicySet elements SHALL be enclosed in a saml/Assertion element wrapper. The saml/Assertion element SHALL be integrity protected.

The policy-user SHALL ignore the xacml/PolicySet@PolicySetId attribute.

The policy-user SHALL verify that the xacml/PolicySet/Target element identifies the wsdl/portType@name attribute of the wsdl/port addressed by the request.

In the case where a policy is wrapped in a saml/Assertion, the host and domain parts of the authenticated name of the originating end-point SHALL be identical to the saml/Assertion@Issuer attribute value. The saml/Assertion@Issuer attribute value SHALL be identical to the CN attribute value in the subject field of the certificate that validates the saml/Assertion element, whether integrity protection is provided by SSL or XML Digital Signature.

If they are present, the policy-user SHALL confirm that the policy is current, by examining the saml/Assertion/Conditions@NotBefore and saml/Assertion/Conditions@NotOnOrAfter attributes.

3. WSDL 1.2

TBD.