3. Indicating Use of WS-Addressing

This specification supports a mechanism for indicating, in a WSDL description, that the endpoint conforms to the WS-Addressing specification. That mechanism uses WS-Policy Framework [*WS Policy 1.5 - Framework*].

3.1 WS-Policy Assertions

The mechanism for indicating that a binding or endpoint conforms to the WS-Addressing specification is through the use of the Web Services Policy - Framework [*WS Policy 1.5 - Framework*] and Web Services Policy - Attachment [*WS Policy 1.5 - Attachment*] specifications. This specification defines three policy assertions.

For WSDL 1.1, these assertions may be attached to `wsdl11:port` or `wsdl11:binding`. For WSDL 2.0, they may be attached to `wsdl20:endpoint` or `wsdl20:binding`.

3.1.1 Addressing Assertion

The wsam:Addressing policy assertion is a nested policy container assertion. The meaning of this assertion, when present in a policy alternative, is that WS-Addressing is required to communicate with the subject. In order to indicate that the subject supports WS-Addressing but does not require its use, an additional policy alternative should be provided which does not contain this assertion. This may be done in WS-Policy compact form by adding the attribute wsp:Optional="true" to the wsam:Addressing assertion.

3.1.2 AnonymousResponses Assertion

The wsam:AnonymousResponses element MAY be used as a policy assertion nested within the wsam:Addressing assertion in accordance with the rules laid down by WS-Policy Framework 1.5 section 4.3.2.

The appearance of this element within a policy alternative indicates that the subject requires any request message that has responses to include response endpoint EPRs that contain the anonymous URI ("http://www.w3.org/2005/08/addressing/anonymous") as the value of [address]. In other words, the subject requires that response instances are sent using the anonymous URI.

The None URI ("http://www.w3.org/2005/08/addressing/none") may appear as the value of [address] in place of the anonymous URI; this value MUST be accepted.

Deleted: endpoint

Deleted: expresses explicit support for

Deleted: s

Deleted: with

Deleted: endpoint

Deleted: guarantees support for

Deleted: responses

Deleted: The absence of the wsam:AnonymousResponses policy assertion within a policy alternative does **not** indicate that the endpoint will not accept request messages with response endpoint EPRs that contain the anonymous URI as an address; it simply indicates the lack of any affirmation of support for anonymous URIs. ¶

3.1.3 NonAnonymousResponses Assertion

The wsam:NonAnonymousResponses element MAY be used as a policy assertion nested within the Addressing assertion in accordance with the rules laid down by WS-Policy Framework 1.5 section 4.3.2.

The appearance of this element within a policy alternative indicates that the subject requires any request message that has responses to include response endpoint EPRs that contain something other than the anonymous URI as the value of [address]. In other words, the subject requires that response instances are sent using a non-anonymous address URI. This assertion is deliberately vague; its presence indicates that some non-anonymous addresses is required for instances of response messages, but doesn't constrain what such an address might look like. A receiver can still reject a request that contains an address that it doesn't understand or that requires a binding it doesn't support.

The None URI ("http://www.w3.org/2005/08/addressing/none") may appear as a non-anonymous address; this value MUST be accepted.

3.1.4 Examples (Compact Form)

Example 3-1. Subject supports WS-Addressing, no statement on supported response EPRs

```
<wsp:Policy>
    <wsam:Addressing wsp:Optional="true">
        <wsp:Policy/>
    </wsam:Addressing>
</wsp:Policy>
```

Example 3-2. Subject requires WS-Addressing, no statement on supported response EPRs

```
<wsp:Policy>
    <wsam:Addressing>
        <wsp:Policy/>
    </wsam:Addressing>
</wsp:Policy>
```

Example 3-4. Subject requires WS-Addressing, requires either anonymous or non-anonymous response EPRs

```
<wsp:Policy>
    <wsam:Addressing>
        <wsp:Policy>
            <wsp:ExactlyOne>
                <wsam:AnonymousResponses/>
                <wsam:NonAnonymousResponses/>
            </wsp:ExactlyOne>
        </wsp:Policy>
    </wsam:Addressing>
</wsp:Policy>
```

Example 3-5. Subject requires WS-Addressing and non-anonymous response EPRs

```
<wsp:Policy>
    <wsam:Addressing>
        <wsp:Policy>
```

Deleted: endpoint expresses explicit support

Deleted: for

Deleted: s

Deleted: with

Deleted: endpoint

Deleted: guarantees

Deleted: support for

Deleted: responses

Deleted: will be accepted

Deleted: As with the other assertions, the absence of the wsam:NonAnonymousResponses policy assertion within a policy alternative does **not** indicate that the endpoint will not accept request messages with response endpoint EPRs that contain something other than the anonymous URI address; it simply indicates the lack of any affirmation of support for them. ¶

Deleted: the value of [address] in place of

Deleted: *Example 3-3. Subject supports WS-Addressing, explicitly (and optionally) supports anonymous and non-anonymous response EPRs*¶

```
<wsp:Policy>¶
    <wsam:Addressing
wsp:Optional="true">¶
        <wsp:Policy>¶

<wsam:AnonymousResponses
wsp:Optional="true"/>¶

<wsam:NonAnonymousResponses
wsp:Optional="true"/>¶
        </wsp:Policy>¶
    </wsam:Addressing>¶
</wsp:Policy>¶
```

Deleted: *explicit support of*

Deleted: *explicit support of*

```
            <wsam:NonAnonymousResponses/>
        </wsp:Policy>
    </wsam:Addressing>
</wsp:Policy>
```

3.1.5 Examples (Normal Form)

Example 3-6. Subject supports WS-Addressing, no statement on supported response EPRs

```
<wsp:Policy>
    <wsp:ExactlyOne>
        <wsp:All/>
        <wsp:All>
            <wsam:Addressing>
                <wsp:Policy>
                    <wsp:ExactlyOne>
                        <wsp:All/>
                    </wsp:ExactlyOne>
                </wsp:Policy>
            </wsam:Addressing>
        </wsp:All>
    </wsp:ExactlyOne>
</wsp:Policy>
```

Example 3-7. Subject requires WS-Addressing, no statement on supported response EPRs

```
<wsp:Policy>
    <wsp:ExactlyOne>
        <wsp:All>
            <wsam:Addressing>
                <wsp:Policy>
                    <wsp:ExactlyOne>
                        <wsp:All/>
                    </wsp:ExactlyOne>
                </wsp:Policy>
            </wsam:Addressing>
        </wsp:All>
    </wsp:ExactlyOne>
</wsp:Policy>
```

Example 3-9. Subject supports WS-Addressing, and requires either anonymous or non-anonymous response EPRs

```
<wsp:Policy>
    <wsp:ExactlyOne>
        <wsp:All>
            <wsam:Addressing>
                <wsp:Policy>
                    <wsp:ExactlyOne>
                        <wsp:All>
                            <wsam:AnonymousResponses/>
                        </wsp:All>
                    </wsp:ExactlyOne>
                </wsp:Policy>
            </wsam:Addressing>
        </wsp:All>
```

Deleted: *8*

Deleted: *explicitly (and optionally) supports*

Deleted: *and*

Deleted:
```
<wsp:Policy>¶
    <wsp:ExactlyOne>¶
        <wsp:All/>¶
        <wsp:All>¶

<wsam:Addressing>¶
                <wsp:Policy>¶

<wsp:ExactlyOne>¶

<wsp:All/>¶

</wsp:ExactlyOne>¶

</wsp:Policy>¶

</wsam:Addressing>¶
        </wsp:All>¶
        <wsp:All>¶

<wsam:Addressing>¶
                <wsp:Policy>¶

<wsp:ExactlyOne>¶

<wsp:All>¶

<wsam:AnonymousResponses/>¶

</wsp:All>¶

</wsp:ExactlyOne>¶

</wsp:Policy>¶

</wsam:Addressing>¶
        </wsp:All>¶
        <wsp:All>¶

<wsam:Addressing>¶
                <wsp:Policy>¶

<wsp:ExactlyOne>¶

<wsp:All>¶

<wsam:NonAnonymousResponses/
>¶

</wsp:All>¶

</wsp:ExactlyOne>¶

</wsp:Policy>¶

</wsam:Addressing>¶
        </wsp:All>¶
        <wsp:All>¶

<wsam:Addressing>¶
                <wsp:Policy>¶

<wsp:ExactlyOne>¶

<wsp:All>¶
```
... [1]

```
        <wsp:All>
            <wsam:Addressing>
                <wsp:Policy>
                    <wsp:ExactlyOne>
                        <wsp:All>
                            <wsam:NonAnonymousResponses/>
                        </wsp:All>
                    </wsp:ExactlyOne>
                </wsp:Policy>
            </wsam:Addressing>
        </wsp:All>
    </wsp:ExactlyOne>
</wsp:Policy>
```

Example 3-10. Subject requires WS-Addressing and non-anonymous response EPRs

Deleted: *explicit support of*

```
<wsp:Policy>
    <wsp:ExactlyOne>
        <wsp:All>
            <wsam:Addressing>
                <wsp:Policy>
                    <wsp:ExactlyOne>
                        <wsp:All>
                            <wsam:NonAnonymousResponses/>
                        </wsp:All>
                    </wsp:ExactlyOne>
                </wsp:Policy>
            </wsam:Addressing>
        </wsp:All>
    </wsp:ExactlyOne>
</wsp:Policy>
```

3.1.6 Finding Compatible Policies

When a client is looking for an endpoint with compatible policy, one common method used is to take the policy intersection between the policy which the client is looking for, and the policy asserted in the WSDL document; a non-empty intersection is sought. The policy used by the client must be written carefully to avoid unexpected results. This is most obvious when the client is not looking for explicit support of a particular kind of response; failing to take care could mean missing a compatible policy.

Consider the following example, where we have a client who does not care whether the endpoint explicitly requires anonymous or non-anonymous responses, and a WSDL for an endppoint which states that the endpoint requires anonymous responses.

Deleted: supports

Deleted: does explicitly

Deleted: support

Example 3-11. Client looking for an endpoint which supports Addressing, WSDL states explicit requirement for anonymous responses

Deleted: *support*

```
<wsp:Policy>
    <wsam:Addressing>
        <wsp:Policy/>
    </wsam:Addressing>
</wsp:Policy>
```

The client's policy (above) states the requirement for Addressing, but no requirement on EPRs used for responses.

```
<wsp:Policy>
    <wsam:Addressing>
        <wsp:Policy>
            <wsam:AnonymousResponses/>
        </wsp:Policy>
    </wsam:Addressing>
</wsp:Policy>
```

The policy attached to the endpoint in the WSDL (above) requires anonymous responses. The intersection of this policy with the client's policy will be empty, so the client will miss a compatible endpoint.

```
<wsp:Policy>
  <wsam:Addressing>
    <wsp:Policy>
      <wsam:AnonymousResponses wsp:Optional="true"/>
    </wsp:Policy>
  </wsam:Addressing>
</wsp:Policy>
```

This is what the client's policy could be; by stating that the wsam:AnonymousResponses assertion is optional, there will be a non-empty intersection with endpoint policies that do and do not contain this assertion.

Deleted: explicit support of

Deleted: states explicit support for

Deleted: Now let us consider a variation on this same situation, where the WSDL marks its explicit support of anonymous responses as ignorable.¶
Example 3-12. Client looking for an endpoint which supports Addressing, WSDL states (ignorable) explicit support for anonymous responses¶

```
<wsp:Policy>¶
  <wsam:Addressing>¶
    <wsp:Policy/>¶
  </wsam:Addressing>¶
</wsp:Policy>¶
```

The client's policy (above) states the requirement for Addressing, but no requirement for explicit support of responses.¶

```
<wsp:Policy>¶
  <wsam:Addressing>¶
    <wsp:Policy>¶
      <wsam:AnonymousResponses wsp:Ignorable="true"/>¶
    </wsp:Policy>¶
  </wsam:Addressing>¶
</wsp:Policy>¶
```

The policy attached to the endpoint in the WSDL (above) states explicit support for anonymous responses, but marks that as an ignorable assertion. Now the result of the policy intersection with the client's policy will depend on whether the client is using lax or strict intersection. The strict intersection of this policy with the client's policy will still be empty. The lax intersection, on the other hand, will not be empty, so the client will find a compatible endpoint.¶
These two examples show the use of wsp:Optional and wsp:Ignorable, and how they can be used to produce non-empty intersections between client and endpoint policies. For more detailed descriptions of the use of wsp:Optional, wsp:Ignorable, and strict and lax intersection, please refer to the WS-Policy Primer [*WS Policy 1.5 - Primer*].¶
¶

```
<wsp:Policy>
    <wsp:ExactlyOne>
        <wsp:All/>
        <wsp:All>
            <wsam:Addressing>
                <wsp:Policy>
                    <wsp:ExactlyOne>
                        <wsp:All/>
                    </wsp:ExactlyOne>
                </wsp:Policy>
            </wsam:Addressing>
        </wsp:All>
        <wsp:All>
            <wsam:Addressing>
                <wsp:Policy>
                    <wsp:ExactlyOne>
                        <wsp:All>
                            <wsam:AnonymousResponses/>
                        </wsp:All>
                    </wsp:ExactlyOne>
                </wsp:Policy>
            </wsam:Addressing>
        </wsp:All>
        <wsp:All>
            <wsam:Addressing>
                <wsp:Policy>
                    <wsp:ExactlyOne>
                        <wsp:All>
                            <wsam:NonAnonymousResponses/>
                        </wsp:All>
                    </wsp:ExactlyOne>
                </wsp:Policy>
            </wsam:Addressing>
        </wsp:All>
        <wsp:All>
            <wsam:Addressing>
                <wsp:Policy>
                    <wsp:ExactlyOne>
                        <wsp:All>
                            <wsam:AnonymousResponses/>
                            <wsam:NonAnonymousResponses/>
                        </wsp:All>
                    </wsp:ExactlyOne>
                </wsp:Policy>
            </wsam:Addressing>
        </wsp:All>
    </wsp:ExactlyOne>
</wsp:Policy>
```

Example 3-9. Subject requires WS-Addressing, requires explicit support of anonymous or non-anonymous response EPRs