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 one policy assertion, and two policy parameters.

Deleted: three

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 may contain policy parameters.. 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.

Deleted: is a nested policy container assertion

Deleted: Assertion

3.1.2 AnonymousResponses Parameter

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

Deleted: assertion

The appearance of this element within a policy alternative indicates that the endpoint expresses explicit support for request messages with 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 endpoint guarantees support for anonymous responses.

The absence of the wsam:AnonymousResponses policy parameter 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.

Deleted: assertion

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.

3.1.3 NonAnonymousResponses Parameter

The wsam:NonAnonymousResponses element MAY be used as a policy parameter 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 endpoint expresses explicit support for request messages with response endpoint EPRs that contain something other than the anonymous URI as the value of [address]. In other words, the endpoint guarantees support for non-anonymous responses. This parameter definition is deliberately vague; its presence indicates that some non-anonymous addresses will be accepted 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.

As with the other policy parameter, the absence of the wsam:NonAnonymousResponses policy parameter 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.

The None URI ("http://www.w3.org/2005/08/addressing/none") may appear as the value of [address] in place of 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>
    </wsam:Addressing>
</wsp:Policy>
```

Example 3-3. Subject supports WS-Addressing, explicitly and supports anonymous and non-anonymous response EPRs

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

Deleted: Assertion

Deleted: assertion

Deleted: assertion

Deleted: assertions

Deleted: assertion

Deleted: <wsp:Policy/>¶

Deleted: *(and optionally)*

Deleted: <wsp:Policy>¶

Deleted: wsp:Optional="true"

Deleted: wsp:Optional="true"

Deleted: ¶ </wsp:Policy>

Example 3-4. Subject requires WS-Addressing, supports anonymous and non-anonymous response EPRs

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

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

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

Example 3-8. Subject supports WS-Addressing, explicitly and supports anonymous and non-anonymous response EPRs

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

Deleted: *requires explicit*

Deleted: *of*

Deleted: *or*

Deleted: ¶
<wsp:Policy>¶
<wsp:ExactlyOne>

Deleted: ¶

</wsp:ExactlyOne>¶
</wsp:Policy>

Deleted: *explicit*

Deleted: ¶
<wsp:Policy>

Deleted: ¶
</wsp:Policy>

Deleted: ¶
<wsp:Policy>¶

<wsp:ExactlyOne>¶

<wsp:All/>¶

</wsp:ExactlyOne>¶

</wsp:Policy>

Deleted: ¶
<wsp:Policy>¶

<wsp:ExactlyOne>¶

<wsp:All/>¶

</wsp:ExactlyOne>¶

</wsp:Policy>

Deleted: *(and optionally)*

Deleted: ¶
<wsp:Policy>¶

<wsp:ExactlyOne>¶

<wsp:All/>¶

</wsp:ExactlyOne>¶

</wsp:Policy>

Deleted: ¶
<wsp:All>¶

<wsam:Addressing>¶
<wsp:Policy>¶

<wsp:ExactlyOne>¶

<wsp:All>¶

<wsam:AnonymousResponses/>¶

</wsp:All>¶

</wsp:ExactlyOne>¶

... [1]

```
</wsp:Policy>
```

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

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

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

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

Deleted: *requires explicit*

Deleted: *of*

Deleted: *or*

Deleted: ¶

```
                <wsp:Policy>¶

<wsp:ExactlyOne>¶

<wsp:All>
```

Deleted: ¶

```
</wsp:All>¶

</wsp:ExactlyOne>¶

</wsp:Policy>¶

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

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

<wsp:ExactlyOne>¶

<wsp:All>
```

Deleted: ¶

```
</wsp:All>¶

</wsp:ExactlyOne>¶

</wsp:Policy>
```

Deleted: *explicit*

Deleted: ¶

```
                <wsp:Policy>¶

<wsp:ExactlyOne>¶

<wsp:All>
```

Deleted: ¶

```
</wsp:All>¶

</wsp:ExactlyOne>¶

</wsp:Policy>
```

Deleted: **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; ¶

… [2]

Page 3: [1] Deleted Tom Rutt 3/6/2007 4:52:00 PM

```
        <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>
```

Page 4: [2] Deleted Tom Rutt 3/6/2007 4:55:00 PM

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 supports anonymous responses, and a WSDL which states that the endpoint does explicitly support anonymous responses.

Example 3-11. Client looking for an endpoint which supports Addressing, WSDL states 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:Policy>

    </wsam:Addressing>

</wsp:Policy>
```

The policy attached to the endpoint in the WSDL (above) states explicit support for 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.

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*].