3 Security Composition Policy

Although it may be possible for an RMS to determine at runtime what supported security composition profiles it may share with an RMD (through, for example, a series of `<wsrm:CreateSequence>` messages that are extended with the `<wsrmsp:SecurityComposition>` element) in general it is operationally more efficient if services can advertise which security composition profiles they support. This information can be used by development, configuration, and component assembly tools to decrease the amount of manual, out-of-band communication necessary to establish reliable, secure message exchanges between two endpoints.

3.1 Security Composition Profile Policy Parameter

The security composition profiles supported by a particular endpoint are advertised by adding one or more `<wsrmsp:SecCompProfile>` elements as parameters to the `<wsrmp:RMAssertion>` policy assertion. The normative outline for this element is:

```
<wsrmsp:SecCompProfile> xs:anyURI </wsrmsp:SecCompProfile>
```

/wsrmsp:SecCompProfile

This element contains an absolute URI that uniquely identifies the supported security composition profile.

3.2 Assertion Example

The following is an example of an RM policy assertion that contains parameters specifying the supported security composition profiles:

```
<wsp:Policy wsu:Id="MyPolicy">
  <wsrmp:RMAssertion>
    <wsrmsp:SecCompProfile>http://docs.oasis-open.org/ws-
rx/wsrmsp/200604/profile/http_auth/samenode</wsrmsp:SecCompProfile>
    <wsrmsp:SecCompProfile>http://docs.oasis-open.org/ws-
rx/wsrmsp/200604/profile/wsc_auth</wsrmsp:SecCompProfile>
  </wsrmp:RMAssertion>

  <!-- omitted assertions -->
</wsp:Policy>
```

Among other things, this policy indicates that WS-ReliableMessaging [WS-RM] must be used. It further indicates that the WS-ReliableMessaging implementation is capable and willing to support the “same-node, TLS/BasicAuth” and “secure conversation” security composition profiles.