Securing RM Sequences

As noted in section 5, an RMS should be able to protect itself against the threat of Sequence Spoofing and/or Sequence Hijacking attacks. One OPTIONAL means of achieving this objective is to include a security token using a `wsse:SecurityTokenReference` element from ~~[~~WS-Security~~]~~ (see section 9 in WS-SecureConversation) in the `CreateSequence` element. This establishes an association between the created (and, if present, offered) Sequence(s) and the referenced security token, such that the RM Source and Destination MUST use the security token as the basis for authorization of all subsequent interactions related to the Sequence(s). The `wsse:SecurityTokenReference` explicitly identifies the token as there may be more than one token on a `CreateSequence` message or inferred from the communication context (e.g. transport protection).

It is RECOMMENDED that a message independent referencing mechanism be used to identify the token, if the token being referenced supports such mechanism.

The following exemplar defines the `CreateSequence` syntax when extended to include a `wsse:SecurityTokenReference`:

```
<wsrm:CreateSequence ...>
    <wsrm:AcksTo ...> wsa:EndpointReferenceType </wsrm:AcksTo>
    <wsrm:Expires ...> xs:duration </wsrm:Expires> ?
    <wsrm:Offer ...>
        <wsrm:Identifier ...> xs:anyURI </wsrm:Identifier>
        <wsrm:Expires ...> xs:duration </wsrm:Expires> ?
        ...
    </wsrm:Offer> ?
    ...
    <wsse:SecurityTokenReference>
      ...
    </wsse:SecurityTokenReference> ?
    ...
</wsrm:CreateSequence>
```

/wsrm:CreateSequence/wsse:SecurityTokenReference

This element uses the extensibility mechanism defined for the wsrm:CreateSequence element (defined in section 3.1) to communicate an explicit reference to the security token, using a wsse:SecurityTokenReference as documented in WS-Security [WSSecurity], that the RM Source and Destination MUST use to authorize messages for the created (and, if present, the offered) Sequence(s). All subsequent messages related to the created (and, if present, the offered) Sequence(s) MUST demonstrate proof-of-rights to the referenced key(e.g., using the key or deriving from the key).

When a RM Source transmits a CreateSequence that has been extended to include a wsse:SecurityTokenReference it ~~should~~SHOULD ensure that the RM Destination both understands and will conform with the requirements listed above. In order to achieve this, the RM Source SHOULD include the UsesSequenceSTR element as a SOAP header block within the CreateSequence message. ~~When t~~This element MUST include~~s~~ a soap:mustUnderstand attribute with a value of 'true'~~,~~. Thus the RM Source can be assured that a RM Destination that responds with a CreateSequenceResponse understands and conforms with the requirements listed above. Note that an RM Destination understanding this header does not mean that it has processed an understood any WS-Security headers, fault behavior defined in WS-Security still applies.

The following exemplar defines the UsesSequenceSTR syntax:

```
<wsrm:UsesSequenceSTR ...>
</wsrm:UsesSequenceSTR>
```

/wsrm:UsesSequenceSTR

This element SHOULD be included as a SOAP header block in <CreateSequence> messages that use the extensibility mechanism described above in this section. ~~If marked with a~~ The soap:mustUnderstand attribute ~~with a~~ value ~~of~~ MUST be 'true'.~~,~~ ~~then t~~The receiving RM Destination MUST understand and correctly implement the extension described above or else generate a soap:MustUnderstand fault, thus aborting the requested Sequence creation.

The following is an example of a CreateSequence message using the wsse:SecurityTokenReference extension and the UsesSequenceSTR header block:

```
<soap:Envelope ...>
  <soap:Header>
      ...
      <wsrm:UsesSequenceSTR soap:mustUnderstand=’true’/>
      ...
  </soap:Header>
  <soap:Body>
    <wsrm:CreateSequence>
      <wsrm:AcksTo>
        <wsa:Address>http://Business456.com/serviceA/789</wsa:Address>
      </wsrm:AcksTo>
      <wsse:SecurityTokenReference>
        ...
      </wsse:SecurityTokenReference>
    </wsrm:CreateSequence>
  </soap:Body>
</soap:Envelope>
```

Sequence STR Assertion

WS-SecurityPolicy [WS-SecurityPolicy] provides a framework and grammar for expressing the security requirements and characteristics of entities in a XML web services based system. The Sequence STR assertion allows the expression of additional security requirements particular to RM sequences to be used in conjunction with WS-SecurityPolicy. Specifically it defines that an RM sequence MUST be bound to an explicit token that is referenced from a wsse:SecurityTokenReference in the CreateSequence message.

This assertion MUST apply to [Endpoint Policy Subject]. The RM Security assertion MUST NOT be used for an endpoint that does not also use the RM assertion.

The normative outline for the Sequence STR Assertion is:

```
<wsrmp:SequenceSTR [wsp:Optional="true"]? ... >
</wsrmp:SequenceSTR >
```

/wsrmp:SequenceSTR

> A policy assertion that specifies security requirements which MUST be used with an RM Sequence that are particular to WS-RM and beyond what can be expressed in WS-SecurityPolicy.

/wsrm:SequenceSTR /@wsp:Optional="true"

Per WS-Policy [WS-Policy], this is compact notation for two policy alternatives, one with and one without the assertion. The intuition is that the behavior indicated by the assertion is optional, or in this case, that the RM Sequence binding to a specific token MAY be used.