Add new section, entitled "Batch Token Requests" following section 4.1, "Requesting a Security Token", as follows:

4.2 Batch Token Requests

There are occasions where efficiency is important. Reducing the number of messages in a message exchange pattern can greatly improve efficiency. One way to do this in the context of WS-Trust is to avoid repeated round-trips for multiple token requests. An example is requesting an identity token as well as tokens that offer other claims in a single batch request operation.

To give an example [Roadmap], imagine an automobile parts supplier that wishes to offer parts to an automobile manufacturer. To interact with the manufacturer web service the parts supplier may have to present a number of tokens, such as an identity token as well as tokens with claims, such as tokens indicating various certifications to meet supplier requirements.

It is possible for the supplier to authenticate to a trust server and obtain an identity token and then subsequently present that token to obtain a certification claim token. However, it may be much more efficient to request both in a single interaction (especially when more than two tokens are required).

Here is an example of a batched authentication request corresponding to this scenario:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Envelope xmlns=http://schemas.xmlsoap.org/soap/envelope/
 xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
 xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
 xmlns:wsp="http://schemas.xmlsoap.org/ws/2002/12/policy"
 xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
 xmlns:wst=" http://docs.oasis-open.org/ws-sx/ws-trust/200512">
<Header>
   <wsse:Security>
      <wsse:UsernameToken Id="user">
        <wsse:Username>person@example.com</wsse:Username>
        <wsse:Password>Apassword</wsse:Password>
      </wsse:UsernameToken>
   </wsse:Security>
</Header>
<Body>

<!-- multiple requests - including identity token and claims token requests -->

<wst:RequestMultipleSecurityTokens>

  <!-- identity token request -->
  <wst:RequestSecurityToken Context="http://www.example.com/1">
     <wst:TokenType>
       http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0
     </wst:TokenType>
     <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/BatchIssue</wst:RequestType>
     <wsp:AppliesTo xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/03/addressing">
        <wsa:EndpointReference>
          <wsa:Address>http://manufacturer.example.com/</wsa:Address>
        </wsa:EndpointReference>
     </wsp:AppliesTo>
     <wsp:PolicyReference URI='http://manufacturer.example.com/IdentityPolicy' />
```

```
34      </wst:RequestSecurityToken>
35
36      <!—certification claim token request -->
37      <wst:RequestSecurityToken Context="http://www.example.com/2">
38         <wst:TokenType>
39          http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0
40         </wst:TokenType>
41         <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-trust/200512 /BatchIssue</wst:RequestType>
42         <wsp:Claims>
43          http://manufacturer.example.com/certification
44         </wsp:Claims>
45         <wsp:PolicyReference URI='http://certificationbody.example.org/certificationPolicy' />
46      </wst:RequestSecurityToken>
47    </wst:RequestMultipleSecurityTokens>
48  </Body>
49  </Envelope>
```

Line #	Description
[020-047]	*RequestMultipleSecurityTokens* is used to encapsulate multiple *RequestSecurityToken* elements
[022-034]	Authentication token request, based on username and password, for manufacturer.example.com, preferably a SAML 2 token.
[036-046]	Certification claim token request, based on the claim of Certification.

4.2.1 Processing Rules

1. The *RequestMultipleSecurityTokens* (RMST) element contains 2 or more *RequestSecurityToken* elements.

2. The single *RequestSecurityTokenResponseCollection* response MUST contain at least one RSTR element corresponding to each RST element in the request. A RSTR element corresponds to an RST element if it has the same Context attribute value as the RST element.

    a. Specifically there is no notion of a deferred response
    b. If any RST request results in an error, then no RSTRs will be returned and a SOAP Fault will be generated as the entire response.

3. Every RST in the request MUST include a Context attribute, and every RSTR in the response MUST reference the appropriate Context value.

4. Every RST in the request MUST use an action URI value in the RequestType element that is a batch version corresponding to the non-batch version, in particular one of the following:

    - http://docs.oasis-open.org/ws-sx/ws-trust/200512 /BatchIssue
    - http://docs.oasis-open.org/ws-sx/ws-trust/200512 /BatchValidate
    - http://docs.oasis-open.org/ws-sx/ws-trust/200512 /BatchRenew
    - http://docs.oasis-open.org/ws-sx/ws-trust/200512 /BatchCancel

These URIs MUST also be used for the [WS-Addressing] actions defined to enable specific processing context to be conveyed to the recipient.

Note that these operations require that the service can either succeed on all the RST requests or must not perform any partial operation.

5. A single authentication mechanism MUST be used for every requested security token in a single message when batch request is used. Thus a single Signature referencing the RSTR in the batch request would be appropriate

    a. No negotiation or other multi-leg authentication mechanisms are allowed when a batch request is used; the communication with STS is limited to one batched-RST request and one RSTRC response.
6. This mechanism requires that every RST in a RMST is to be handled by the single endpoint processing the RMST.

4.3 Batched Response

A single *RequestSecurityTokenResponseCollection* element is used to contain all of the *RequestSecurityTokenResponse* responses corresponding to the single *RequestMultipleSecurityTokens* element in the corresponding request. Either a SOAP Fault is returned or a *RequestSecurityTokenResponse* containing a RSTR element corresponding to each RST request. There is no notion of a deferred response.

Every RSTR MUST have a Context attribute with the value given in the corresponding RST element.

Here is a sample response corresponding to the sample request above:

```
<?xml version="1.0" encoding="utf-8" ?>
<Envelope xmlns=http://schemas.xmlsoap.org/soap/envelope/
 xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
 xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
 xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512"
 xmlns:wsp="http://schemas.xmlsoap.org/ws/2002/12/policy"
 xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
<Header>
</Header>
<Body>
<wst:RequestSecurityTokenResponseCollection>

  <!—identity token – authentication completed -->
  <wst:RequestSecurityTokenResponse Context="http://www.example.com/1">
    <wst:TokenType>
      http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0
    </wst:TokenType>

    <wsp:AppliesTo xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/03/addressing">
      <wsa:EndpointReference>
        <wsa:Address>http://manufacturer.example.com/</wsa:Address>
      </wsa:EndpointReference>
    </wsp:AppliesTo>

    <wst:LifeTime><wsu:Created>2005-04-11T06:26:59Z</wsu:Created>
```

```
26      <wsu:Expires>2005-04-12T06:26:59Z</wsu:Expires></wst:LifeTime>
27
28      <wst:RequestedSecurityToken>
29        … SAML 2 assertion to indicate authentication achieved…
30       </wst:RequestedSecurityToken>
31    </wst:RequestSecurityTokenResponse>
32
33    <wst:RequestSecurityTokenResponse Context="http://www.example.com/2">
34      <wst:TokenType>
35        http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0
36      </wst:TokenType>
37
38      <wst:LifeTime><wsu:Created>2005-04-11T06:26:59Z</wsu:Created>
39      <wsu:Expires>2005-04-12T06:26:59Z</wsu:Expires></wst:LifeTime>
40
41      <wst:RequestedSecurityToken>
42        … SAML 2 assertion to indicate certification achieved…
43      </wst:RequestedSecurityToken>
44
45    </wst:RequestSecurityTokenResponse>
46  </wst:RequestSecurityTokenResponseCollection>
47  </Body>
48  </Envelope>
```

Line #	Description
[011-046]	A *RequestSecurityTokenResponseCollection* element containing multiple *RequestSecurityTokenReponse*'s.
[013-031]	Token indicating successful authentication
[033-045]	Claim token to indicate that certification has been achieved.

If an error occurs in the processing of a single request, a SOAP Fault MUST be generated for the entire batch request, so no RSTR elements will be returned in this case.

[Roadmap] Security in a Web Services World: A Proposed Architecture and Roadmap, A joint security whitepaper from IBM Corporation and Microsoft Corporation. April 7, 2002, Version 1.0