4 Syntax of the Secured SOAP Document

In this section, we present the syntax of the secured SOAP document; that is, X_s and R_s in Figure 3. First, the secured SOAP document can follow the syntax defined in WS-Security [12]. Since WS-Security employs the XML encryption and XML signature specifications, and XML encryption does not support attribute encryption, we cannot perform attribute encryption. Figure 19 and Figure 20 show a SOAP message and its corresponding secured version obtained in WS-Security. Note that the cipher values of some elements in Figure 20 have been removed. The corresponding WSSL document used to activate the securing procedure is shown in Figure 36 in Appendix A.

Attribute encryption can be used to secure the SOAP message in the syntax of an encrypted element defined in the DSL [9,10,11] (see Figure 37 in Appendix A). Beside, the complete XML files of those codes are listed in Appendix A

```
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2001/12/soap-envelope">
  <soapenv:Header />
  <soapenv:Body>
    <transaction>
      <credit_info>
        <CardNumber>0000-0000-0000</CardNumber>
        <ExpiryDate>2007-6-20</ExpiryDate>
        <Issuer>TEST</Issuer>
      </credit_info>
      <order_info orederDate="2006-06-01">
        <person_info>
          <RegisterID>TACO</RegisterID>
```

```
            <Name>Chang</Name>
            <Address>Taipei</Address>
            <Phone>0958444888</Phone>
          </person_info>
          <Book id="sp0001">
           <BookName>Web services security</BookName>
           <OrderAmount>1</OrderAmount>
          </Book>
        </order_info>
      </transaction>
  </soapenv:Body>
</soapenv:Envelope>
```

Figure 19: A requested SOAP message before encryption and signing

```
<soapenv:Envelope xmlns:ds=http://www.w3.org/2000/09/xmldsig#
                  xmlns:soapenv="http://www.w3.org/2001/12/soap-envelope"
                  xmlns:wsu="http://schemas.xmlsoap.org/ws/2003/06/utility"
                  xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
 <soapenv:Header>
  <wsse:Security xmlns:wsse="http://schemas.xmlsoap.org/ws/2003/06/secext">
   <ds:Signature>
    <ds:SignedInfo>
     <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
     <ds:SignatureMethod
          Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
     <ds:Reference URI="#request_sign-0">
      <ds:Transforms>
       <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      </ds:Transforms>
      <ds:DigestMethod
```

```
                    Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
      <ds:DigestValue>ZTGM4B+fNPnZWVPw1aHM=</ds:DigestValue>
     </ds:Reference>
    </ds:SignedInfo> <ds:SignatureValue>u4BkXkBll2BoMu4wGs…[2]=</ds:SignatureValue>
    <ds:KeyInfo>
     <wsse:SecurityTokenReference>
      <wsse:KeyIdentifier EncodingType="#Base64Binary" ValueType="#X509v3">
       MIIDXn9NYJtFE3mrw0izhXvwMwcTVdlwYGjcwsbztjZcw==
      </wsse:KeyIdentifier>
     </wsse:SecurityTokenReference>
    </ds:KeyInfo>
   </ds:Signature>
   <xenc:ReferenceList>
    <xenc:DataReference URI="#request_pattern1" />
    <xenc:DataReference URI="#request_pattern2" />
   </xenc:ReferenceList>
  </wsse:Security>
</soapenv:Header>
<soapenv:Body wsu:id="request_sign-0">
 <transaction>
   <xenc:EncryptedData Type=http://www.w3.org/2001/04/xmlenc#Element
                       wsu:Id="request_pattern1">
   <xenc:EncryptedMethod
                      Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />
    <xenc:CipherData>
     <xenc:CipherValue>erVtqvyzk8QboR5nX4… </xenc:CipherValue>
    </xenc:CipherData>
   </xenc:EncryptedData>
   <order_info orederDate="2006-06-01">
      <xenc:EncryptedData Type=http://www.w3.org/2001/04/xmlenc#Element
```

[2] The cipher data in this element is too long to be included, and hence it is removed.

```
                                wsu:Id="request_pattern2">
        <xenc:EncryptedMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />
        <xenc:CipherData>
          <xenc:CipherValue>Pjj63lIHm7Q07fRg5…</xenc:CipherValue>
        </xenc:CipherData>
       </xenc:EncryptedData>
       <Book id="sp0001">
        <BookName>Web services security</BookName>
        <OrderAmount>1</OrderAmount>
       </Book>
    </order_info>
  </transaction>
 </soapenv:Body>
</soapenv:Envelope>
```

Figure 20: A requested SOAP message after encryption and signing in WS-Security