

Note: WSS Encryption Example – SOAP body, SOAP Body and SwA Attachment

Frederick Hirsch, Nokia
August 18, 2004

This note gives a detailed example of encrypting the SOAP body and then an example encrypting both the SOAP body and a SwA attachment. The purpose is to expose assumptions and potential ambiguities in the SOAP Message Security Specification. This is a non-normative document intended for discussion (the choice of steps here are not necessarily those of an implementation).

1. Encrypting Primary SOAP Message Body (no SwA attachment)

Assume the following initial SOAP message:

```
<S11:Envelope
  xmlns:S11="http://schemas.xmlsoap.org/soap/envelope/"
  <S11:Header>
  </S11:Header>
  <S11:Body>
    some items
  </S11:Body>
</S11:Envelope>
```

To encrypt the SOAP body content (encrypting the body element itself is not allowed according to WSS) the following steps are outlined in the WSS specification:

a) Create a Security header

This also implies adding the wsse namespace declaration.

```
<S11:Envelope
  xmlns:S11="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
  wsswssecurity-secext-1.0.xsd">
  <S11:Header>
    <wsse:Security>
    </wsse:Security>
  </S11:Header>
  <S11:Body>
    some items
  </S11:Body>
</S11:Envelope>
```

b) Create an EncryptedKey element in this security header.

This is used to convey the symmetric key used for the XML Encryption of the body, encrypted with another key, typically an asymmetric key. Note that ED will be an id on the EncryptedData element to be created in the next step.

```

47 <S11:Envelope
48   xmlns:S11="http://schemas.xmlsoap.org/soap/envelope/"
49   xmlns:wssse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
50 wsswssecurity-secext-1.0.xsd"
51   xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
52   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
53
54   <S11:Header>
55     <wsse:Security>
56       <xenc:EncryptedKey Id='EK'>
57         <EncryptionMethod
58           Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
59         <CipherData><CipherValue>xyzabc</CipherValue></CipherData>
60         <ReferenceList>
61           <DataReference URI='#ED' />
62         </ReferenceList>
63       </EncryptedKey>
64     </wsse:Security>
65   </S11:Header>
66   <S11:Body>
67     some items
68   </S11:Body>
69 </S11:Envelope>
70

```

71 c. Provide KeyInfo for key used to encrypt the symmetric key.

72 In this example an X.509 WSS token is used to convey information about a public-private
73 key pair

```

74 <S11:Envelope
75   xmlns:S11="http://schemas.xmlsoap.org/soap/envelope/"
76   xmlns:wssse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
77 wsswssecurity-secext-1.0.xsd"
78   xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
79   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
80
81   <S11:Header>
82     <wsse:Security>
83       <wsse:BinarySecurityToken wsu:Id="Acert"
84         EncodingType="http://docs.oasis-
85 open.org/wss/2004/01/oasis-200401-wss-soap-message-security-
86 1.0#Base64Binary"
87         ValueType="http://docs.oasis-
88 open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
89 1.0#x509v3">
90         ...
91       </wsse:BinarySecurityToken>
92
93       <xenc:EncryptedKey Id='EK'>
94         <EncryptionMethod
95           Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
96         <ds:KeyInfo Id="keyinfo">
97           <wsse:SecurityTokenReference>
98             <ds:X509Data>
99               <ds:X509IssuerSerial>
100                 <ds:X509IssuerName>
101                   DC=ACMECorp, DC=com
102                 </ds:X509IssuerName>
103                 <ds:X509SerialNumber>12345678</X509SerialNumber>
104               </ds:X509IssuerSerial>

```

```

105         </ds:X509Data>
106         </wsse:SecurityTokenReference>
107     </ds:KeyInfo>
108     <CipherData><CipherValue>xyzabc</CipherValue></CipherData>
109     <ReferenceList>
110         <DataReference URI='#ED' />
111     </ReferenceList>
112 </EncryptedKey>
113 </wsse:Security>
114 </S11:Header>
115 <S11:Body>
116     some items
117 </S11:Body>
118 </S11:Envelope>
119

```

120 d) Replace content of body with EncryptedData element.

121

- 122 • Encrypt the content of the SOAP Body element according to XML encryption and
- 123 replace that content with an EncryptedData element.
- 124 • Include an Id attribute with the value specified in the EncryptedKey DataReference, in
- 125 this case "ED".
- 126 • Note that the CipherData element contains a CipherValue element containing the
- 127 ciphertext corresponding to the original SOAP body content.
- 128 • Note that WSS does not require including a KeyInfo in the EncryptedData element,
- 129 since the key is indicated by a reference in the security header. This is not shown in the
- 130 core examples, and not used here.
- 131 • We assume no explicit ReferenceList child element of wsse:Security is required when
- 132 an EncryptedKey ReferenceList is used.

```

133 <S11:Envelope
134     xmlns:S11="http://schemas.xmlsoap.org/soap/envelope/"
135     xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
136 wsswssecurity-secext-1.0.xsd"
137     xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
138     xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
139
140     <S11:Header>
141         <wsse:Security>
142
143             <wsse:BinarySecurityToken wsu:Id="Acert"
144                 EncodingType="http://docs.oasis-
145 open.org/wss/2004/01/oasis-200401-wss-soap-message-security-
146 1.0#Base64Binary"
147                 ValueType="http://docs.oasis-
148 open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
149 1.0#x509v3">
150                 ...
151             </wsse:BinarySecurityToken>
152
153             <xenc:EncryptedKey Id='EK'>
154                 <EncryptionMethod
155                     Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
156                 <ds:KeyInfo Id="keyinfo">
157                     <wsse:SecurityTokenReference>
158                         <ds:X509Data>
159                             <ds:X509IssuerSerial>

```

```

160         <ds:X509IssuerName>
161             DC=ACMECorp, DC=com
162         </ds:X509IssuerName>
163         <ds:X509SerialNumber>12345678</X509SerialNumber>
164     </ds:X509IssuerSerial>
165 </ds:X509Data>
166 </wsse:SecurityTokenReference>
167 </ds:KeyInfo>
168 <CipherData><CipherValue>xyzabc</CipherValue></CipherData>
169 <ReferenceList>
170     <DataReference URI='#ED' />
171 </ReferenceList>
172 </EncryptedKey>
173
174 </wsse:Security>
175 </S11:Header>
176 <S11:Body>
177     <xenc:EncryptedData Id='ED'
178         <xenc:EncryptionMethod
179             Algorithm='http://www.w3.org/2001/04/xmlenc#aes128-cbc' />
180     <xenc:CipherData>
181         <xenc:CipherValue>DEADBEEF</xenc:CipherValue>
182     </xenc:CipherData>
183 </xenc:EncryptedData>
184 </S11:Body>
185 </S11:Envelope>

```

2. Encrypting Primary SOAP Message Body and SwA attachment, using same symmetric key

Now assume the need is to encrypt both the SOAP message body and a SwA attachment using the same symmetric key and to convey this key using an EncryptedKey element.

Add a new Processing rule to the SwA profile: Process the attachments first. This is to have a correct order of elements in the wsse:Security header, specifically that a receiver encounters the EncryptedKey before the EncryptedData for the attachment.

Assume the following multipart-MIME SwA message:

```

197 Content-Type: multipart/related; boundary="arggh" type=text/xml
198 --arggh
199 Content-Type: text/xml
200
201 <S11:Envelope
202     xmlns:S11="http://schemas.xmlsoap.org/soap/envelope/">
203     <S11:Header>
204     </S11:Header>
205     <S11:Body>
206         some items
207     </S11:Body>
208 </S11:Envelope>
209 --arggh
210 Content-Type: image/png
211 Content-Id: <bar>
212 Content-Transfer-Encoding: base64
213
214 the image
215

```

- a. Create a Security header and place an EncryptedData element for the attachment in the header.
- b. Encrypt the content of the attachment, replacing the content with the cipherdata, and refer to this from the EncryptedData element using a CipherReference.

```
Content-Type: multipart/related; boundary="arggh" type=text/xml
--arggh
Content-Type: text/xml

<S11:Envelope
  xmlns:S11="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:wssse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wsswssecurity-secext-1.0.xsd">
  <S11:Header>
    <wsse:Security>
      <xenc:EncryptedData
        Id='EA'
        Type="http://docs.oasis-open.org/wss/2004/XX/oasis-2004XX-
wss-swa-profile-1.0#Attachment-Content-Only"
        MimeType="image/png">
        <xenc:EncryptionMethod
          Algorithm='http://www.w3.org/2001/04/xmlenc#aes128-cbc' />
        <xenc:CipherData>
          <xenc:CipherReference URI=cid:bar">
            <ds:Transforms>
              <ds:Transform Algorithm="http://docs.oasis-
open.org/wss/2004/XX/oasis-2004XX-wss-swa-profile-1.0#Attachment-
Content-Only-Transform"/>
            </ds:Transforms>
          </xenc:CipherReference>
        </xenc:CipherData>
      </xenc:EncryptedData>
    </wsse:Security>
  </S11:Header>
  <S11:Body>
    some items
  </S11:Body>
</S11:Envelope>
--arggh
Content-Type: application/octet-stream
Content-Id: <bar>
Content-Transfer-Encoding: base64

CIPHERDATA
```

- c. Now follow the same steps as outlined above for encrypting the SOAP message body, with the modification that the ReferenceList for the EncryptedKey should also include the EncryptedData element added to the header for the attachment.

The final result will look like:

```

271 Content-Type: multipart/related; boundary="arggh" type=text/xml
272 --arggh
273 Content-Type: text/xml
274
275 <S11:Envelope
276     xmlns:S11="http://schemas.xmlsoap.org/soap/envelope/"
277     xmlns:wss="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
278 wsswssecurity-secext-1.0.xsd"
279     xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
280     xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
281
282     <S11:Header>
283         <wsse:Security>
284
285             <wsse:BinarySecurityToken wsu:Id="Acert"
286                 EncodingType="http://docs.oasis-
287 open.org/wss/2004/01/oasis-200401-wss-soap-message-security-
288 1.0#Base64Binary"
289                 ValueType="http://docs.oasis-
290 open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
291 1.0#x509v3">
292                 ...
293             </wsse:BinarySecurityToken>
294
295             <xenc:EncryptedKey Id='EK'>
296                 <EncryptionMethod
297                     Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
298                 <ds:KeyInfo Id="keyinfo">
299                     <wsse:SecurityTokenReference>
300                         <ds:X509Data>
301                             <ds:X509IssuerSerial>
302                                 <ds:X509IssuerName>
303                                     DC=ACMECorp, DC=com
304                                 </ds:X509IssuerName>
305                                 <ds:X509SerialNumber>12345678</X509SerialNumber>
306                             </ds:X509IssuerSerial>
307                         </ds:X509Data>
308                     </wsse:SecurityTokenReference>
309                 </ds:KeyInfo>
310                 <CipherData><CipherValue>xyzabc</CipherValue></CipherData>
311                 <ReferenceList>
312                     <DataReference URI='#EA' />
313                     <DataReference URI='#ED' />
314                 </ReferenceList>
315             </EncryptedKey>
316
317             <xenc:EncryptedData
318                 Id='EA'
319                 Type="http://docs.oasis-open.org/wss/2004/XX/oasis-2004XX-
320 wss-swa-profile-1.0#Attachment-Content-Only"
321                 MimeType="image/png">
322                 <xenc:EncryptionMethod
323                     Algorithm='http://www.w3.org/2001/04/xmlenc#aes128-cbc' />
324                 <xenc:CipherData>
325                     <xenc:CipherReference URI=cid:bar">
326                         <ds:Transforms>
327                             <ds:Transform Algorithm="http://docs.oasis-
328 open.org/wss/2004/XX/oasis-2004XX-wss-swa-profile-1.0#Attachment-
329 Content-Only-Transform"/>
330                         </ds:Transforms>
331                     </xenc:CipherReference>
332                 </xenc:CipherData>
333             </xenc:EncryptedData>
334

```

```
335     </wsse:Security>
336 </S11:Header>
337 <S11:Body>
338   <xenc:EncryptedData Id='ED'
339     <xenc:EncryptionMethod
340       Algorithm='http://www.w3.org/2001/04/xmlenc#aes128-cbc' />
341     <xenc:CipherData>
342       <xenc:CipherValue>DEADBEEF</xenc:CipherValue>
343     </xenc:CipherData>
344   </xenc:EncryptedData>
345 </S11:Body>
346 </S11:Envelope>
347 --arggh
348 Content-Type: application/octet-stream
349 Content-Id: <bar>
350 Content-Transfer-Encoding: base64
351
352 CIPHERDATA
353
```