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.

```
<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"
  xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
  xmls:ds="http://www.w3.org/2000/09/xmldsig#">

  <S11:Header>
   <wsse:Security>
     <xenc:EncryptedKey Id='EK'>
       <EncryptionMethod
         Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
      <CipherData><CipherValue>xyzabc</CipherValue></CipherData>
      <ReferenceList>
        <DataReference URI='#ED'/>
      </ReferenceList>
     </EncryptedKey>
   </wsse:Security>
  </S11:Header>
  <S11:Body>
   some items
  </S11:Body>
</S11:Envelope>
```

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

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

```
<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"
  xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
  xmls:ds="http://www.w3.org/2000/09/xmldsig#">

 <S11:Header>
   <wsse:Security>
     <wsse:BinarySecurityToken wsu:Id="Acert"
           EncodingType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-soap-message-security-
1.0#Base64Binary"
           ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#x509v3">
       ...
     </wsse:BinarySecurityToken>

     <xenc:EncryptedKey Id='EK'>
       <EncryptionMethod
         Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
      <ds:KeyInfo Id="keyinfo">
        <wsse:SecurityTokenReference>
          <ds:X509Data>
            <ds:X509IssuerSerial>
              <ds:X509IssuerName>
               DC=ACMECorp, DC=com
              </ds:X509IssuerName>
               <ds:X509SerialNumber>12345678</X509SerialNumber>
            </ds:X509IssuerSerial>
```

```
          </ds:X509Data>
        </wsse:SecurityTokenReference>
      </ds:KeyInfo>
      <CipherData><CipherValue>xyzabc</CipherValue></CipherData>
      <ReferenceList>
        <DataReference URI='#ED'/>
      </ReferenceList>
    </EncryptedKey>
  </wsse:Security>
 </S11:Header>
 <S11:Body>
  some items
 </S11:Body>
</S11:Envelope>
```

d) Replace content of body with EncryptedData element.

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

```
<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"
  xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
  xmls:ds="http://www.w3.org/2000/09/xmldsig#">

 <S11:Header>
   <wsse:Security>

     <wsse:BinarySecurityToken wsu:Id="Acert"
           EncodingType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-soap-message-security-
1.0#Base64Binary"
           ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#x509v3">
       ...
     </wsse:BinarySecurityToken>

     <xenc:EncryptedKey Id='EK'>
       <EncryptionMethod
         Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
      <ds:KeyInfo Id="keyinfo">
        <wsse:SecurityTokenReference>
          <ds:X509Data>
            <ds:X509IssuerSerial>
```

```
              <ds:X509IssuerName>
               DC=ACMECorp, DC=com
              </ds:X509IssuerName>
               <ds:X509SerialNumber>12345678</X509SerialNumber>
            </ds:X509IssuerSerial>
          </ds:X509Data>
        </wsse:SecurityTokenReference>
      </ds:KeyInfo>
      <CipherData><CipherValue>xyzabc</CipherValue></CipherData>
      <ReferenceList>
        <DataReference URI='#ED'/>
      </ReferenceList>
     </EncryptedKey>

   </wsse:Security>
  </S11:Header>
  <S11:Body>
   <xenc:EncryptedData Id='ED'
    <xenc:EncryptionMethod
     Algorithm='http://www.w3.org/2001/04/xmlenc#aes128-cbc'/>
    <xenc:CipherData>
     <xenc:CipherValue>DEADBEEF</xenc:CipherValue>
    </xenc:CipherData>
  </xenc:EncryptedData>
 </S11:Body>
</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 EncyrptedData for the attachment.

Assume the following multipart-MIME SwA message:

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

<S11:Envelope
 xmlns:S11="http://schemas.xmlsoap.org/soap/envelope/">
  <S11:Header>
  </S11:Header>
  <S11:Body>
   some items
  </S11:Body>
</S11:Envelope>
--arggh
Content-Type: image/png
Content-Id: <bar>
Content-Transfer-Encoding: base64

the image
```

a. Create a Security header and 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:wsse="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:

```
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:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wsswssecurity-secext-1.0.xsd"
  xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
  xmls:ds="http://www.w3.org/2000/09/xmldsig#">

 <S11:Header>
   <wsse:Security>

     <wsse:BinarySecurityToken wsu:Id="Acert"
           EncodingType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-soap-message-security-
1.0#Base64Binary"
           ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#x509v3">
       ...
     </wsse:BinarySecurityToken>

     <xenc:EncryptedKey Id='EK'>
       <EncryptionMethod
         Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
      <ds:KeyInfo Id="keyinfo">
        <wsse:SecurityTokenReference>
          <ds:X509Data>
            <ds:X509IssuerSerial>
              <ds:X509IssuerName>
               DC=ACMECorp, DC=com
              </ds:X509IssuerName>
               <ds:X509SerialNumber>12345678</X509SerialNumber>
            </ds:X509IssuerSerial>
          </ds:X509Data>
        </wsse:SecurityTokenReference>
      </ds:KeyInfo>
      <CipherData><CipherValue>xyzabc</CipherValue></CipherData>
      <ReferenceList>
        <DataReference URI='#EA'/>
        <DataReference URI='#ED'/>
      </ReferenceList>
     </EncryptedKey>

     <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>
   <xenc:EncryptedData Id='ED'
    <xenc:EncryptionMethod
     Algorithm='http://www.w3.org/2001/04/xmlenc#aes128-cbc'/>
    <xenc:CipherData>
     <xenc:CipherValue>DEADBEEF</xenc:CipherValue>
    </xenc:CipherData>
  </xenc:EncryptedData>
 </S11:Body>
</S11:Envelope>
--arggh
Content-Type: application/octet-stream
Content-Id: <bar>
Content-Transfer-Encoding: base64

CIPHERDATA
```