6.1 General Considerations

Encryption of the <Assertion>, <BaseID>, <NameID> and <Attribute> elements is provided by use of XML Encryption [XMLEnc]. Encrypted data and optionally one or more encrypted keys MUST replace the plaintext information in the same location within the XML instance. The <xenc:EncryptedData> element's Type attribute SHOULD be used and, if it is present, MUST have the value http://www.w3.org/2001/04/xmlenc#Element.

Any of the algorithms defined for use with XML Encryption MAY be used to perform the encryption. The SAML schema is defined so that the inclusion of the encrypted data yields a valid instance.

6.2 Key and Data Referencing Guidelines

If an encrypted key is NOT included in the XML instance, then the relying party must be able to locally determine the decryption key, per [XMLEnc].

Implementations of SAML MAY implicitly associate keys with the corresponding data they are used to encrypt, through the positioning of <xenc:EncryptedKey> elements next to the associated <xenc:EncryptedData> element, within the enclosing SAML parent element. However, the following set of explicit referencing guidelines are suggested to facilitate interoperability.

If the encrypted key is included in the XML instance, then it SHOULD be referenced within the associated <xenc:EncryptedData> element, or alternatively embedded within the <xenc:EncryptedData> element. When an <xenc:EncryptedKey> element is used, the <ds:KeyInfo> element within <xenc:EncryptedData> SHOULD reference the <xenc:EncryptedKey> element using a <ds:RetrievalMethod> element of Type http://www.w3.org/2001/04/xmlenc#EncryptedKey.

In addition, an <xenc:EncryptedKey> element SHOULD contain an <xenc:ReferenceList> element containing a <xenc:DataReference> that references the corresponding <xenc:EncryptedData> element(s) that the key was used to encrypt.

In scenarios where the encrypted element is being “multicast” to multiple recipients, and the key used to encrypt the message must be in turn encrypted individually and independently for each of the multiple recipients, the <xenc:CarriedKeyName> element SHOULD be used to assign a common name to each of the <xenc:EncryptedKey> elements so that a <ds:KeyName> can be used from within the <xenc:EncryptedData> element’s <ds:KeyInfo> element.

Within the <xenc:EncryptedData> element, the <ds:KeyName> can be thought of as an ”alias” that is used for backwards referencing from the <xenc:CarriedKeyName> element in each individual <xenc:EncryptedKey> element. While this accommodates a “multicast” approach, each recipient must be able to understand (at least one) <ds:KeyName>. The Recipient attribute is used to provide a hint as to which key is meant for which recipient.

The SAML implementation has the discretion to accept or reject a message where multiple `Recipient` attributes or `<ds:KeyName>` elements are understood. It is RECOMMENDED that implementations simply use the first key they understand and ignore any additional keys.

6.3 Examples

In the following example, the parent element (`<EncryptedID>`) contains `<xenc:EncryptedData>` and (referenced) `<xenc:EncryptedKey>` elements as siblings (note that the key can in fact be anywhere in the same instance, and the key references the `<xenc:EncryptedData>` element) :

```
<saml:EncryptedID xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
      <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
            Id="Encrypted_DATA_ID"
            Type="http://www.w3.org/2001/04/xmlenc#Element">
            <xenc:EncryptionMethod
                  Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig">
                  <ds:RetrievalMethod URI="#Encrypted_KEY_ID"
                  Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"/>
            </ds:KeyInfo>
            <xenc:CipherData>
                  <xenc:CipherValue>Nk4W4mx...</xenc:CipherValue>
            </xenc:CipherData>
      </xenc:EncryptedData>

      <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
            Id="Encrypted_KEY_ID"
            <xenc:EncryptionMethod
                  Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
            <xenc:CipherData>
                  <xenc:CipherValue>PzA5X...</xenc:CipherValue>
            </xenc:CipherData>
            <xenc:ReferenceList>
                  <xenc:DataReference URI="#Encrypted_DATA_ID"/>
            </xenc:ReferenceList>
      </xenc:EncryptedKey>
</saml:EncryptedID>
```

In the following `<EncryptedAttribute>` example, the `<xenc:EncryptedKey>` element is contained within the `<xenc:EncryptedData>` element, so there is no explicit referencing:

```
<saml:EncryptedAttribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
      <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
            Id="Encrypted_DATA_ID"
            Type="http://www.w3.org/2001/04/xmlenc#Element">
            <xenc:EncryptionMethod
                  Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                  <xenc:EncryptedKey Id="Encrypted_KEY_ID">
                        <xenc:EncryptionMethod
                  Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
                        <xenc:CipherData>
                              <xenc:CipherValue>SDFSDF... </xenc:CipherValue>
                        </xenc:CipherData>
```

```
                  </xenc:EncryptedKey>
            </ds:KeyInfo>
            <xenc:CipherData>
                  <xenc:CipherValue>Nk4W4mx...</xenc:CipherValue>
            </xenc:CipherData>
      </xenc:EncryptedData>
</saml:EncryptedAttribute>
```

The final example shows an assertion encrypted for multiple recipients, using the `<xenc:CarriedKeyName>` approach:

```
<saml:EncryptedAssertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
      <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
            Id="Encrypted_DATA_ID"
            Type="http://www.w3.org/2001/04/xmlenc#Element">
            <xenc:EncryptionMethod
                  Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                  <ds:KeyName>MULTICAST_KEY_NAME</ds:KeyName>
            </ds:KeyInfo>
            <xenc:CipherData>
                  <xenc:CipherValue>Nk4W4mx...</xenc:CipherValue>
            </xenc:CipherData>
      </xenc:EncryptedData>

      <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
            Id="Encrypted_KEY_ID_1" Recipient="https://sp1.org"
            <xenc:EncryptionMethod
                  Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                  <ds:KeyName>KEY_NAME_1</ds:KeyName>
            </ds:KeyInfo>
            <xenc:CipherData>
                  <xenc:CipherValue>xyzABC...</xenc:CipherValue>
            </xenc:CipherData>
            <xenc:ReferenceList>
                  <xenc:DataReference URI="#Encrypted_DATA_ID"/>
            </xenc:ReferenceList>
            <xenc:CarriedKeyName>MULTICAST_KEY_NAME</xenc:CarriedKeyName>
      </xenc:EncryptedKey>

      <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
            Id="Encrypted_KEY_ID_2" Recipient="https://sp2.org">
            <xenc:EncryptionMethod
                  Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                  <ds:KeyName>KEY_NAME_2</ds:KeyName>
            </ds:KeyInfo>
            <xenc:CipherData>
                  <xenc:CipherValue>abcXYZ...</xenc:CipherValue>
            </xenc:CipherData>
            <xenc:ReferenceList>
                  <xenc:DataReference URI="#Encrypted_DATA_ID"/>
            </xenc:ReferenceList>
            <xenc:CarriedKeyName>MULTICAST_KEY_NAME</xenc:CarriedKeyName>
      </xenc:EncryptedKey>
```

```
</saml:EncryptedAssertion>
```