Encryption proposal

Definitions:
A ***compartment*** is a set of message elements with identical access policy.

A compartment is identified with a symmetric key, and is represented by an <wsse:compartment> element. The <wsse:compartment> element SHALL contain a set of <xenc:EncryptedKey> elements, one for the symmetric key encrypted under each key-agreement key. It SHALL also contain a set of <xenc:DataReference> elements containing the ID or XPath reference to each of the message elements in the compartment. Because each message element is only encrypted once (with one symmetric key), no message element SHALL appear in more than one <wsse:compartment> element.

<wsse:compartment> elements SHALL be contained in the <wsse:Security> element that omits the S:role attribute.

Each recipient is represented by a <ds:KeyInfo> element containing a reference to its key-agreement certificate.

References flow …

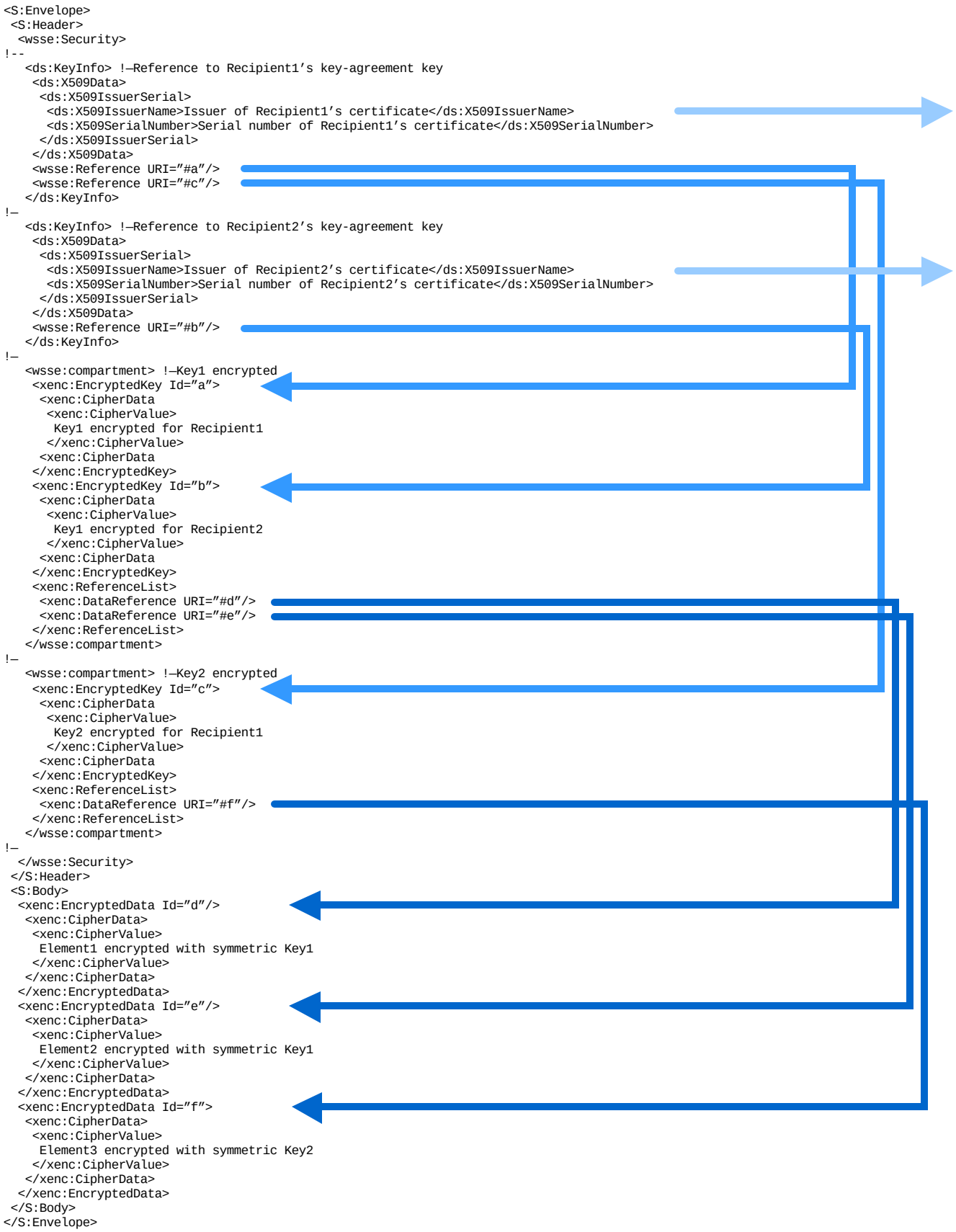
ds:KeyInfo -> Compartment -> message element

Then the receiving processor …

1 - identifies any references to its own keys in <ds:KeyInfo> elements,
2 – from these elements, it identifies any <wsse:compartment> elements for which it can decrypt the symmetric key,
3 – from these elements, it identifies any message elements for which it can decrypt the contents.

There follows an illustrative example. It implements the policy:

Recipient 1 is permitted access to Element 1, Element 2 and Element 3. Recipient 2 is permitted access to Element 1 and Element 2 only.


<S:Envelope>
<S:Header>
<wsse:Security>
!--
<ds:KeyInfo> !—Reference to Recipient1’s key-agreement key
<ds:X509Data>
<ds:X509IssuerSerial>
<ds:X509IssuerName>Issuer of Recipient1’s certificate</ds:X509IssuerName>
<ds:X509SerialNumber>Serial number of Recipient1’s certificate</ds:X509SerialNumber>
</ds:X509IssuerSerial>
</ds:X509Data>
<wsse:Reference URI=”#a”/>
<wsse:Reference URI=”#c”/>
</ds:KeyInfo>
!—
<ds:KeyInfo> !—Reference to Recipient2’s key-agreement key
<ds:X509Data>
<ds:X509IssuerSerial>
<ds:X509IssuerName>Issuer of Recipient2’s certificate</ds:X509IssuerName>
<ds:X509SerialNumber>Serial number of Recipient2’s certificate</ds:X509SerialNumber>
</ds:X509IssuerSerial>
</ds:X509Data>
<wsse:Reference URI=”#b”/>
</ds:KeyInfo>
!—
<wsse:compartment> !—Key1 encrypted
<xenc:EncryptedKey Id=”a”>
<xenc:CipherData
<xenc:CipherValue>
Key1 encrypted for Recipient1
</xenc:CipherValue>
<xenc:CipherData
</xenc:EncryptedKey>
<xenc:EncryptedKey Id=”b”>
<xenc:CipherData
<xenc:CipherValue>
Key1 encrypted for Recipient2
</xenc:CipherValue>
<xenc:CipherData
</xenc:EncryptedKey>
<xenc:ReferenceList>
<xenc:DataReference URI=”#d”/>
<xenc:DataReference URI=”#e”/>
</xenc:ReferenceList>
</wsse:compartment>
!—
<wsse:compartment> !—Key2 encrypted
<xenc:EncryptedKey Id=”c”>
<xenc:CipherData
<xenc:CipherValue>
Key2 encrypted for Recipient1
</xenc:CipherValue>
<xenc:CipherData
</xenc:EncryptedKey>
<xenc:ReferenceList>
<xenc:DataReference URI=”#f”/>
</xenc:ReferenceList>
</wsse:compartment>
!—
</wsse:Security>
</S:Header>
<S:Body>
<xenc:EncryptedData Id=”d”/>
<xenc:CipherData>
<xenc:CipherValue>
Element1 encrypted with symmetric Key1
</xenc:CipherValue>
</xenc:CipherData>
</xenc:EncryptedData>
<xenc:EncryptedData Id=”e”/>
<xenc:CipherData>
<xenc:CipherValue>
Element2 encrypted with symmetric Key1
</xenc:CipherValue>
</xenc:CipherData>
</xenc:EncryptedData>
<xenc:EncryptedData Id=”f”>
<xenc:CipherData>
<xenc:CipherValue>
Element3 encrypted with symmetric Key2
</xenc:CipherValue>
</xenc:CipherData>
</xenc:EncryptedData>
</S:Body>
</S:Envelope>