Changes Made To SKSML v1.0 Committee Specification v1.0

Editor: Anil Saldhana, Red Hat Inc.

Summary of Changes

The EKMI TC agreed that the core SKSML specification should not require neither SOAP nor Web Services Security. So this update is essentially to remove the specification needs of SOAP/WSS.

Section : Abstract

Replaced the line:

> SKSML messages are transported within a SOAP layer, protected by a Web Services Security (WSS) header and can be used over standard HTTP securely.

With:

> SKSML messages are transported securely over standard HTTP using XML Security (XML Signature and XML Encryption).

Section: 2.1 Requirements (non-normative)

Replaced the following line:

- SKSML uses SOAP and XML for encapsulating its requests and responses and can thus, be used on any platform that supports these two underlying protocols;

With:

- SKSML uses XML for encapsulating its requests and responses and can thus, be used on any platform that supports XML;

Replaced the following line:

- SKSML relies on the Web Services Security (WSS) standard 1.0, which in turn supports the use of XML Signature and XML Encryption within the SOAP Header. Relying only the on the WSS profile that uses RSA cryptographic key-pairs and digital certificates, SKSML uses the digital signatures for authenticity and message-integrity, while using RSA-encryption for confidentiality;

With:

- SKSML relies on XML Signature and XML Encryption. Relying only the on the WSS profile that uses RSA cryptographic key-pairs and digital certificates, SKSML uses the digital signatures for authenticity and message-integrity, while using RSA-encryption for confidentiality;

Section: 3.1 Request for a new symmetric key

Removed the following lines:

While the ***SymkeyRequest*** element is very simple, the Web Service Security (WSS) envelope – which provides security for all SKSML messages – expands the size of the message. The same request shown above, is displayed below in its entirety, with its WSS envelope. Please note that some content – such as Base64-encoded binary content - has been reformatted for aesthetics and clarity of the XML elements. The actual elements and data-types have been preserved from actual SKSML messages.
For an interpretation of the XML elements shown below, please refer to **[WSS]**.
For the sake of brevity, this specification will dispense with showing the SOAP envelope and the WSS elements in all other examples, when discussing SKSML.

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header>
       <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" SOAP-ENV:mustUnderstand="1">
       <wsse:BinarySecurityToken xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd"
             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" wsu:Id="XWSSGID-1172790302111-1738806553">
             MIIDfDCCAmSgAwIBAgIIAe/AvliGc3AwDQYJKoZIhvcNAQELBQAwZzEmMCQGA1UEAxMdU3Ryb25nab
          S2V5IERFTU8gU3Vib3JkaW5hdGUgQ0ExJDAiBgNVBAsTG0ZvciBTdHJvbmdLZXkgREVNTyBVc2Ug1d
   T25seTEXMBUGA1UEChMOU3Ryb25nQXV0aCBJbmMwHhcNMDYwNzI1MTcxMDMwWhcNMDcwNzIa64dd3k
   A1UECxMbRm9yIFN0cm9uZ0tleSBERU1PIFVzZSBPbmx5MRcwFQYDVQQKEw5TdHJvbmdBdXRoIEl2da
   S2V5IERFTU8gU3Vib3JkaW5hdGUgQ0ExJDAiBgNVBAsTG0ZvciBTdHJvbmdLZXkgREVNTyBVc2Ugia
   T25seTEXMBUGA1UEChMOU3Ryb25nQXV0aCBJbmMwHhcNMDYwNzI1MTY0NjEwWhcNMDcwNzI1s34wdd
   NjEwWjBpMREwDwYKCZImiZPyLGQBARMBOTEVMBMGA1UEAxMMU0tTIFNlcnZlci0xMSQwIgYDVQsdw2
   ExtGb3IgU3Ryb25nS2V5IERFTU8gVXNlIE9ubHkxFzAVBgNVBAoTDlN0cm9uZ0F1dGggSW5jMIIBd2
          NBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAztppqRoU5A8plxx1Rz1QEUnlAAM1D5g9+isIr3wxa
   hbwjtFSMYilnY4iV77xU/nsMOnMZ7RxsLYKdCzQ1ODVYqQwqmAvaJ5Z6SVy34gZ51YG+rSWE3NjFsd
   bOXW8RJYA/Tn6Lmht/qngrcaqqmtP0cAAiMRZOWtCTmC2K/LEqDabXSyU6Hh8ySNE3njybvmWpresf
   zsYokTdvnWQqT6tKo1OwJsdJ1+hxM7DrnMLvMNq5reINfsKhDdX17wzhrBUx+hiYA/qo8tMXkL6wsd
          4PN5dYugtzpSzIdUO5tIg58Avhzwo7hy5oofBlKFY22CeljQ36u0bMjuyGj6UYHs3rdfdfsds32rda
   YzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAyAmxMZhYA8wHJ4UE4b61s51JVWe4Fygj4MCf3a
   hvcNAQELBQADggEBACK05PtvZD4WPglOe=
             </wsse:BinarySecurityToken>
         <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                   <ds:SignedInfo>
             <ds:CanonicalizationMethod
                                  Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                   <InclusiveNamespaces
                                  xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
                                  PrefixList="wsse SOAP-ENV"/>
              </ds:CanonicalizationMethod>
                         <ds:SignatureMethod
                                  Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1"/>
                         <ds:Reference URI="#XWSSGID-1172790300636-653454040">
             <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
```

```
            <ds:DigestValue>lU4m+rp4oebgl9g+t3nRaZYqUlE=</ds:DigestValue>
                        </ds:Reference>
              <ds:Reference URI="#XWSSGID-1172790300637708871805">
              <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>

            <ds:DigestValue>WCpOmTCbffcEHXhGf5rlEYWLrZg=</ds:DigestValue>
                        </ds:Reference>
                    </ds:SignedInfo>
                    <ds:SignatureValue>

            svStAvBRRrF+g2biPl7uWHkJTQPIl8t4phMbOZQsZlQcn36tcMSj/a4+4LPNfOB3Y8yO2lr1Oa1

            fGqCPAWZNuEH34VQEM196rRwV258mgp8uwpXEYJIgPJqg89w8+/NdaODccLQ2Bizu7QM/HSM2ab
                    ogNJwqmbSyIazOsnOcU=
                    </ds:SignatureValue>
                <ds:KeyInfo>
                  <wsse:SecurityTokenReference xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
                           wsu:Id="XWSSGID-1172790300633-442423344">
                              <wsse:Reference URI="#XWSSGID-1172790302111-1738806553"
                                             ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"/>
                              </wsse:SecurityTokenReference>
                    </ds:KeyInfo>
              </ds:Signature>
          <wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-1172790300637708871805">
                    <wsu:Created>2007-03-01T23:05:00Z</wsu:Created>
                    <wsu:Expires>2007-03-01T23:05:05Z</wsu:Expires>
              </wsu:Timestamp>
            </wsse:Security>
     </SOAP-ENV:Header>
     <SOAP-ENV:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-1172790300636-653454040">
              <ekmi:SymkeyRequest
                    xmlns:ekmi="http://docs.oasis-open.org/ekmi/2008/01">
                    <ekmi:GlobalKeyID>10514-0-0</ekmi:GlobalKeyID>
              </ekmi:SymkeyRequest>
            </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Section: 3.2 : Response with a new symmetric key

The following line has been removed:
(The SOAP message, as indicated earlier, is secured using WSS, but only the actual SKSML content is displayed and discussed here).

Section 3.3 : Request for an existing symmetric key

The following line has been removed:
(The SOAP message is secured using WSS, but only the actual SKSML content is displayed and discussed here).

Section 3.8: Response with multiple new symmetric keys

The following line has been removed:
Additionally, the SOAP message, as indicated earlier, is secured using WSS, but only the actual SKSML content is displayed and discussed here.

Section 3.14 Request for a symmetric key-caching policy

The following lines has been removed:
For an interpretation of the XML elements shown below, please refer to **[WSS]**.
For the sake of brevity, this specification will dispense with showing the SOAP envelope and the WSS elements in all other examples, when discussing SKSML.

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header>
       <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" SOAP-ENV:mustUnderstand="1">
       <wsse:BinarySecurityToken xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd"
             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" wsu:Id="XWSSGID-1172790302111-1738806553">
             MIIDfDCCAmSgAwIBAgIIAe/AvliGc3AwDQYJKoZIhvcNAQELBQAwZzEmMCQGA1UEAxMdU3Ryb25nab
      S2V5IERFTU8gU3Vib3JkaW5hdGUgQ0ExJDAiBgNVBAsTG0ZvciBTdHJvbmdLZXkgREVNTyBVc2Ug1d
      T25seTEXMBUGA1UEChMOU3Ryb25nQXV0aCBJbmMwHhcNMDYwNzI1MTcxMDMwWhcNMDcwNzIa64dd3k
      A1UECxMbRm9yIFN0cm9uZ0tleSBERU1PIFVzZSBPbmx5MRcwFQYDVQQKEw5TdHJvbmdBdXRoIEl2da
      S2V5IERFTU8gU3Vib3JkaW5hdGUgQ0ExJDAiBgNVBAsTG0ZvciBTdHJvbmdLZXkgREVNTyBVc2Ugia
      T25seTEXMBUGA1UEChMOU3Ryb25nQXV0aCBJbmMwHhcNMDYwNzI1MTY0NjEwWhcNMDcwNzI1s34wdd
      NjEwWjBpMREwDwYKCZImiZPyLGQBARMBOTEVMBMGA1UEAxMMU0tTIFNlcnZlci0xMSQwIgYDVQsdw2
      ExtGb3IgU3Ryb25nS2V5IERFTU8gVXNlIE9ubHkxFzAVBgNVBAoTDlN0cm9uZ0F1dGggSW5jMIIBd2
             NBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAztppqRoU5A8plxx1Rz1QEUnlAAM1D5g9+isIr3wxa
      hbwjtFSMYilnY4iV77xU/nsMOnMZ7RxsLYKdCzQ1ODVYqQwqmAvaJ5Z6SVy34gZ51YG+rSWE3NjFsd
      bOXW8RJYA/Tn6Lmht/qngrcaqqmtP0cAAiMRZOWtCTmC2K/LEqDabXSyU6Hh8ySNE3njybvmWpresf
      zsYokTdvnWQqT6tKo1OwJsdJ1+hxM7DrnMLvMNq5reINfsKhDdX17wzhrBUx+hiYA/qo8tMXkL6wsd

4PN5dYugtzpSzIdUO5tIg58Avhzwo7hy5oofBlKFY22CeljQ36u0bMjuyGj6UYHs3rdfdfsds32rda
      YzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAyAmxMZhYA8wHJ4UE4b61s51JVWe4Fygj4MCf3a
      hvcNAQELBQADggEBACK05PtvZD4WPglOe=
             </wsse:BinarySecurityToken>
       <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                   <ds:SignedInfo>
             <ds:CanonicalizationMethod
                                    Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                   <InclusiveNamespaces
                                    xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
                                    PrefixList="wsse SOAP-ENV"/>
              </ds:CanonicalizationMethod>
                         <ds:SignatureMethod
                                    Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1"/>
                         <ds:Reference URI="#XWSSGID-1172790300636-653454040">
              <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>

           <ds:DigestValue>lU4m+rp4oebgl9g+t3nRaZYqUlE=</ds:DigestValue>
                         </ds:Reference>
              <ds:Reference URI="#XWSSGID-117279030063770887l805">
              <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>

           <ds:DigestValue>WCpOmTCbffcEHXhGf5rlEYWLrZg=</ds:DigestValue>
                         </ds:Reference>
```

```
                    </ds:SignedInfo>
                    <ds:SignatureValue>

          svStAvBRRrF+g2biPl7uWHkJTQPIl8t4phMbOZQsZlQcn36tcMSj/a4+4LPNfOB3Y8yO2lr1Oa1

          fGqCPAWZNuEH34VQEM196rRwV258mgp8uwpXEYJIgPJqg89w8+/NdaODccLQ2Bizu7QM/HSM2ab
                    ogNJwqmbSyIazOsnOcU=
                    </ds:SignatureValue>
          <ds:KeyInfo>
             <wsse:SecurityTokenReference xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
                       wsu:Id="XWSSGID-1172790300633-442423344">
                          <wsse:Reference URI="#XWSSGID-1172790302111-1738806553"
                                         ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"/>
                       </wsse:SecurityTokenReference>
                    </ds:KeyInfo>
             </ds:Signature>
       <wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-117279030063770887l805">
                    <wsu:Created>2007-03-01T23:05:00Z</wsu:Created>
                    <wsu:Expires>2007-03-01T23:05:05Z</wsu:Expires>
             </wsu:Timestamp>
          </wsse:Security>
   </SOAP-ENV:Header>
   <SOAP-ENV:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-1172790300636-653454040">
....

          </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Added [n03] -[n05] to include a XML Digital Signature block.

Section 3.15 Response with a symmetric key-caching policy (1)

The following line has been removed:
(The SOAP message, as indicated earlier, is secured using WSS, but only the actual SKSML content is displayed and discussed here).

Section 4.1 Element <SymkeyRequest>

Removed the following line:
While it is a top-level element within this specification, a `<SymkeyRequest>` element MUST be enclosed within a ***SOAP Body*** element of a ***SOAP Envelope*** to conform to the security requirements of this specification. The ***SOAP Header*** of the ***SOAP Envelope*** MUST enclose a ***Security*** element conforming to **[WSS]** with a ***ValueType*** attribute containing the value http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3. The ***Security*** element must conform to all other requirements of the specified security profile in **[WSS]** to form a well-formed, secure message.

Section 4.6 Element <SymkeyResponse>

Removed the following lines:
While <SymkeyResponse> is a top-level element within this specification, it MUST be enclosed within a ***SOAP Body*** element of a ***SOAP Envelope*** to conform to the security requirements of this specification. The ***SOAP Header*** of the ***SOAP Envelope*** MUST enclose a ***Security*** element conforming to **[WSS]** with a ***ValueType*** attribute containing the value http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3. The ***Security*** element must conform to all other requirements of the specified security profile in **[WSS]** to form a well-formed, secure message.

Section 4.9 Element <SymkeyError>

The following lines removed:
When a request for a symmetric key fails despite successfully being processed by the SOAP layer, there MUST be at least one <SymkeyError> element in a <SymkeyResponse> element. When a <SymkeyRequest> fails at the SOAP layer, the response SHALL consist of a ***SOAPFault***.

Section 4.25 Element <KeyCachePolicyRequest>

The following lines removed:
While it is a top-level element within this specification, a **<SymkeyRequest>** element MUST be enclosed within a ***SOAP Body*** element of a ***SOAP Envelope*** to conform to the security requirements of this specification. The ***SOAP Header*** of the ***SOAP Envelope*** MUST enclose a ***Security*** element conforming to **[WSS]** with a ***ValueType*** attribute containing the value http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3. The ***Security*** element must conform to all other requirements of the specified security profile in **[WSS]** to form a well-formed, secure message.

Replaced the following lines:
The **<KeyCachePolicyRequest>** has no child elements. The SOAP Header of the signed request provides the **SKS** server with all the information it needs to process the request: the identity of the requester, strong authentication and message integrity of the request.

With:
The **<KeyCachePolicyRequest>** has one child element. The child element has the XML Digital signature that can help the server with the identity of the requester, strong authentication and message integrity of the request.

Section 4.29 Use of Web Services Security (WSS)

Replace “MUST” with “MAY”

Section 5 Bindings

A short section inserted.

Section 6 Conformance

Previously it was section 5.