BSP 1.1 Scenario Architecture

Technical requirements for securing the SCM Sample Application

Document Status: Final Material

Current Edition: BSP1.1 Architecture Final Material

Date: January 19, 2010

Editors:
Salim Zeitouni, IBM
Monica J. Martin, Microsoft

Administrative contact:
secretary@ws-i.org

1.1 Status of This Document

This document is a Final Material of the BSP 1.1 scenario Architecture document developed by the WS-I Sample Applications team. The members of the WS-I Sample Application team will appreciate comments and suggestions. These should be sent by email to the WS-I Sample Apps WG Mailing List.

1.2 Notice

1.3 Feedback

The Web Services-Interoperability Organization (WS-I) would like to receive input, suggestions and other feedback ("Feedback") on this work from a wide variety of industry participants to improve its quality over time.

By sending email, or otherwise communicating with WS-I, you (on behalf of yourself if you are an individual, and your company if you are providing Feedback on behalf of the company) will be deemed to have granted to WS-I, the members of WS-I, and other parties that have access to your Feedback, a non-exclusive, non-transferable, worldwide, perpetual, irrevocable, royalty-free license to use, disclose, copy, license, modify, sublicense or otherwise distribute and exploit in any manner whatsoever the Feedback you provide regarding the work. You acknowledge that you have no expectation of confidentiality with respect to any Feedback you provide. You represent and warrant that you have rights to provide this Feedback, and if you are providing Feedback on behalf of a company, you represent and warrant that you have the rights to provide Feedback on behalf of your company. You also acknowledge that WS-I is not required to review, discuss, use, consider or in any way incorporate your Feedback into future versions of its work. If WS-I does incorporate some or all of your Feedback in a future version of the work, it may, but is not obligated to include your name (or, if you are identified as acting on behalf of your company, the name of your company) on a list of contributors to the work. If the foregoing is not acceptable to you and any company on whose behalf you are acting, please do not provide any Feedback.

Feedback on this document should be directed to wsi_samples_comment@mp.ws-i.org.

Table of Contents

Revision History

Date	Version ID	Who	Comments
25 August 2008	1	Salim Zeitouni(IBM)	Document creation
10 September 2008	2	Monica Martin(MSFT)	Editorial comments & addition of overview section
18 September 2008	3	Salim Zeitouni (IBM)	Editorial updates
22 September 2008	4	Salim Zeitouni (IBM)	Clarify Test Methodology
1 October 2008	5	Salim Zeitouni (IBM) Monica Martin (MSFT)	Scenario Updates for security requirements
8 October 2008	6	Salim Zeitouni (IBM)	Add Assertion map to scenarios
21 May 2009	7	Salim Zeitouni (IBM) Monica J. Martin (MS)	Editorial comments during review for Working Group Draft
28 May 2009	8	Salim Zeitouni (IBM)	Approved as Working Group Draft.
9 July 2009	9	Monica J. Martin (MS)	Added an optional Scenario 4 (variation of Scenario 2), Signature Confirmation with Encrypted Signature scenario approved 6/17/2009 by SAWG.
15 July 2009	10	Salim Zeitouni (IBM)	Approved as Working Group Draft.
03 Septmenber 2009	11	Salim Zeitouni (IBM)	Refine Test methodology based on the testing done with these simple echo-like scenarios.
14 September 2009	12	Monica J. Martin (MS)	Integrated changes to scenarios based on BSP 1.1 profile revisions in draft. Added sample messages and comments from SAWG call and review 9/10.
15 September 2009	13	Monica J. Martin (MS)	Correct reference for algorithm method.
19 September 2009	14	Monica J. Martin (MS)	SAWG approved editor's draft with minor editorial changes first as Working Group Draft and then simultaneously as Working Group Approval Draft
30 September 2009	15	Monica J. Martin (MS)	Corrected requirement references.
1 October 2009	16	Monica J. Martin (MS)	Corrected BSP public page link until WGAD BSP 1.1 is published.
22 October 2009	17	Monica J. Martin (MS)	Approved as Board Approval Draft.
15 December 2009	18	Monica J. Martin (MS)	Approved as Approval Draft.
19 January 2010	19	Monica J. Martin (MS)	Approved by the membership and WS-I Board.

Copyright

Confidentiality

2 Introduction to the WS-I Scenarios for Basic Security Profile 1.1

2.1 Purpose

This document describes the architecture of the WS-I scenarios that supports the Basic Security Profile version 1.1 [BSP11].

Its purpose is to:

- Provide a common architecture and design document for companies that develop sample applications demonstrating the interoperability of the Basic Security Profile.

2.2 Objective

The main objectives of the WS-I in developing a BSP 1.1 sample scenarios are to:

- Demonstrate the wire-level interoperability of messages between applications, developed on platforms from multiple vendors that each conform to the Basic Security Profile version 1.1.
- Discover practical implementation challenges associated with developing applications that conform to the Basic Security Profile version 1.1. This information can then be provided to the BSP team to consider revising and improving the Basic Security Profile, as required, to promote interoperability.

These key architectural objectives focus on how Web services adhering to the WS-I *Basic Security Profile Version 1.1* might be modeled, rather than demonstrating Web services security best practices.

2.3 Pre-Requisites

To fully understand this document, the reader should understand the following:

- The Basic Security Profile version 1.1 [BSP11]
- The Basic Security Profile version 1.0 [BSP10]
- SCM Security Architecture [SCMSA]

The reader should also be familiar with the general principles and concepts of:

- Developing applications that use web services.
- Securing data using cryptographic and other security techniques.

3 Testing Overview

The WS-I Basic Security Profile version 1.0 provides a strong foundation for the development of secure, yet interoperable Web services. Basic Security Profile version 1.1 builds on the Basic Security Profile version 1.0 strong foundation.

The following lists some of the standards that BSP 1.1 Profile incorporates.

- Web Services Security: SOAP Message Security 1.1 (WS-Security 2004) OASIS Standard Specification, 1 February 2006 –“ http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf”
- Transport Layer Mechanisms - "http://ws-i.org/profiles/basic-security/1.1/transport"
- Username Token - "http://ws-i.org/profiles/basic-security/1.1/username-token"
- X.509 Certificate Token - "http://ws-i.org/profiles/basic-security/1.1/x.509-certificate-token"
- REL Token - "http://ws-i.org/profiles/basic-security/1.1/rel-token"
- Kerberos Token - "http://ws-i.org/profiles/basic-security/1.1/kerberos-token"
- SAML Token - "http://ws-i.org/profiles/basic-security/1.1/saml-token"
- Attachment Security - "http://ws-i.org/profiles/basic-security/1.1/swa"

Core to BSP, Web Services Security 1.1 specification (WSS 1.1) introduced interesting new features that WS-I determined clarifications were needed to ensure interoperability. The new features highlighted by the BSP 1.1 are:

- Encrypted SOAP Header
- Signature Confirmation
- Thumbprint Reference

The newly added scenarios for BSP 1.1 work to exercise these features and ensure that BSP 1.1 assertions are compliant.

The previous test methodology was simplified. Instead of redeveloping the Sample Application to test the various profile assertions for the BSP 1.1 profile, an echo-like request-response scenario was used. One service and corresponding Web Service client were created to expose elements to exercise the BSP 1.1 assertions. Based on this one service, several scenarios were created to test the three new features (Encrypted SOAP Header, Signature Confirmation, and Thumbprint Reference). An additional optional scenario labeled Scenario 4 is also included to test the feature of Signature Confirmation. The new test methodology exercises the three features mentioned here and uses functionality consistent with BSP 1.0 Sample Application to drive other BSP 1.0/1.1 test assertions. With this approach, both the new features in BSP 1.1, and existing functionality defined in BSP 1.0 and which remains in BSP 1.1 are covered.

The new scenarios are based on a common service called MessageService, see the WSDL of MessageService. For more new scenario details, see Appendix D.

4 Summary of BSP 1.1 requirement

BSP 1.1 built on the capabilities and constraints defined in BSP 1.0. In BSP 1.1, requirements surrounding Signature Confirmation, Security Tokens Reference and Encrypted Headers were defined to support WSS 1.1 specification and token profiles. These new or revised requirements served as the core basis to scope the BSP 1.1 scenarios. A brief overview of the primary requirements tested in the BSP 1.1 scenarios are found in the following table.

Table 1: BSP 1.1 scenarios mapping to core BSP 1.1 requirements

Scenario	BSP 1.1 Section	BSP 1.1 Requirement
Scenario 1 (Encrypted Header)	Section 6.1.1	R3212
Scenario 1 (Encrypted Header)	Section 10.1	R3228
Scenario 1 (Encrypted Header)	Section 10.1	R3230
Scenario 1 (Encrypted Header)	Section 10.5.2	R5627
Scenario 1 (Encrypted Header)	Section 10.1	R3232
Scenario 1 (Encrypted Header)	Section 10.5.2	R5624
Scenario 1 (Encrypted Header)	Section 10.7	R5608
Scenario 1 (Encrypted Header)	Section 10.8	R3006
Scenario 1 (Encrypted Header)	Section 10.13	R5614
Scenario 2 (Signature Confirmation)	Section 9.11	R5441
Scenario 3 (Thumbprint Reference)	Section 13.2.6	R5206
Scenario 4 (Signature Confirmation) [optional scenario]	Section 9.11	R5441

5 Summary of scenarios Quality of Service (QoS)

Table 1 provides a summary of the requirements for message integrity, confidentiality, and Algorithm used for each of the Request and Response methods of the various BSP scenarios. Each Operation request/response is a hyperlink to the part of this document that describes the security associated with that operation and an example of a complete message.

Table 2: Summary of QoS for the BSP 1.1 scenarios

Scenario	Operation request/response	Message Integrity	Confidentiality	Algorithm
MessageService with no QoS	MessageService Request	None	None	None
MessageService with no QoS	MessageService Response	None	None	None
Scenario 1	a. Encrypted SOAP Header: Request (wsu:Id for EncryptedHeader element)	X509:Body, Timestamp, msgHeaderElement	msgHeaderElement, Body	Key: RSA 1.5, Data: AES 128, Digest: SHA1
Scenario 1	b. Encrypted SOAP Header: Response (wsu:Id for EncryptedHeader element)	X509:Body, Timestamp	Body	Key: RSA 1.5, Data: AES 128, Digest: SHA1
Scenario 1	c. Encrypted SOAP Header: Request	X509:Body, Timestamp, msgHeaderElement	msgHeaderElement, Body	Key: RSA 1.5, Data: AES 128, Digest: SHA1
Scenario 1	d. Encrypted SOAP Header: Response	X509:Body, Timestamp	Body	Key: RSA 1.5, Data: AES 128, Digest: SHA1
Scenario 2	Signature Confirmation Request	X509: Body, Timestamp	Body,	Key: RSA 1.5, Data: AES 128, Digest: SHA1
Scenario 2	Signature Confirmation Response	X509:Body, Timestamp, Signature Confirmation	Body	Key: RSA 1.5, Data: AES 128, Digest: SHA1
Scenario 3	Thumbprint Reference Request	X509:Body, Timestamp	Body, Thumbprint Reference	Key: RSA 1.5, Data: AES 128, Digest: SHA1
Scenario 3	Thumbprint Reference Response	X509:Body, Timestamp	Body, Thumbprint Reference	Key: RSA 1.5, Data: AES 128, Digest: SHA1
(optional scenario) Scenario 4	Signature Confirmation Request with Encrypted Signature	X509: Body, Timestamp	Body, Signature	Key: RSA 1.5, Data: AES 128, Digest: SHA1
(optional scenario) Scenario 4	Signature Confirmation Response with Encrypted Signature and Encrypted Signature Confirmation	X509:Body, Timestamp, Signature Confirmation	Body, Signature, Signature Confirmation	Key: RSA 1.5, Data: AES 128, Digest: SHA1

The following provides an explanation of each column of the table.

5.1 Message Integrity

This column consists of entries of the following form:

Certificate ":" MessageParts

Certificate contains the public key that identifies whose private key was used to sign various parts of the message. It consists of two parts:

Certificate Type. This always contains "X.509" and identifies that an X.509 certificate is being used.

MessageParts is a list of the different parts of the message that are signed and appear as separate items in the signature manifest.

5.2 Confidentiality

Confidentiality indicates whether or not the message is encrypted. It contains one of the following:

"None". The security analysis concluded that confidentiality was not required

MessageParts. *Message Parts* are a list of the parts of the message that are encrypted.

5.3 Algorithm

If the message is signed or encrypted, then the Algorithm column describes the cryptographic algorithms used. Its structure is as follows:

"Key:" Asymmetric Algorithm [", Data:" Symmetric Algorithm] ", Digest:" Secure Hash Algorithm

Asymmetric Algorithm identifies the algorithm used to generate public/private key pairs. It is used to generate and verify signatures as well as to encrypt and decrypt the symmetric key used to encrypt and decrypt the message content. It always contains "RSA 1.5" which indicates that the RSA 1.5 Encryption standard for creating signatures is being used – see ftp://ftp.rsasecurity.com/pub/pkcs/ascii/pkcs-1.asc

Symmetric Algorithm identifies the algorithm used for encrypting and decrypting the message content. It contains "AES 128" (indicating 128 bit key size).

Secure Hash Algorithm identifies the algorithm used for calculating the unique fingerprint for each of the signed parts of the message. It always contains "SHA1" as described in the Secure Hash Standard – see http://www.itl.nist.gov/fipspubs/fip180-1.htm

6 Scenarios Overview

These three scenarios use the Message Service WSDL, and Message Service Request and Response to exercise new or changed BSP 1.1 requirements. The three scenarios are:

1. Encrypted Header Message Service Request and Response
2. Signature Confirmation Message Service Request and Response
3. Thumbprint Reference Scenario Message Service Request and Response
4. (optional scenario) Signature Confirmation with EncryptedSignature Message Service Request and Response

6.1 Encrypted Header

Basic128Rsa15 algorithm suite is used for this request-response scenario to exercise the Encrypted Header and Encrypted Data requirements. For example, Scenario 1 exercises the case wherein EncryptedHeader element is used for the data reference for the encryption step (using the wsu:Id).

1. Message Service Request encrypts the Header Element (SOAP Header) and then the Body.
2. Request signs Timestamp, Body and the Header Element.
3. Message Service Response encrypts the Body and signs Timestamp and Body.

Note:

- The encrypted ReferenceList respectively uses the Encrypted Header wsu:Id or EncryptedData id within the Encrypted Header to reference the encryption.
- No signature encryption is used.
- The same MessageProtectionOrder, EncryptBeforeSign, is used to encrypt and then sign the Message Service Request and Response.

Below you find links to the SOAP requests and responses:

Encrypted SOAP Header: Request (wsu:Id for EncryptedHeader element)
Encrypted SOAP Header Response (wsu:Id for EncryptedHeader element)

Encrypted SOAP Header: Request
Encrypted SOAP Header: Response

6.2 Signature Confirmation

Using the same Basic128Rsa15 algorithm suite, this request-response scenario exercises the Signature Confirmation requirements.

1. Message Service Request signs the Timestamp, Body and then encrypts the Body.
2. Message Service Response signs the Timestamp, Body and then encrypts the Body. The Response includes a signed Signature Confirmation.
3. The Signature Confirmation element contains a wsu:Id attribute so that it can be referenced.

Note:

- No signature encryption is used.
- The same MessageProtectionOrder, SignBeforeEncrypt, is used to sign then encrypt the Message Service Request and Response.

Below you find links to the SOAP request and response:

Signature Confirmation Request
Signature Confirmation Response

6.3 Thumbprint Reference

Using the same Basic128Rsa15 algorithm suite, this request-response scenario exercises the use of the Thumbprint Reference in the EncryptedKey KeyInfo.

1. Message Service Request references the EncryptedKey KeyInfo using the Thumbprint Reference.
2. Security Token reference that references the X509_TOKEN has an appropriate ValueType attribute
3. Request also signs Timestamp, Body and then encrypts Body.
4. Message Service Response signs Timestamp, Body and then encrypts Body.

Note:

- No signature encryption is used.
- The same MessageProtectionOrder, SignBeforeEncrypt, is used to sign then encrypt the Message Service Request and Response.

Below you find links to the SOAP request and response:

Thumbprint Reference Request
Thumbprint Reference Response

6.4 Signature Confirmation with Encrypted Signature (optional scenario)

Using the same Basic128Rsa15 algorithm suite, this optional request-response scenario exercises the Signature Confirmation requirements using an EncryptedSignature.

4. Message Service Request signs the Timestamp, Body and then encrypts the entire Signature and the Body.
5. Message Service Response signs the Timestamp, Body and then encrypts the entire Signature, the Body and the Signature Confirmation.

Note:

- Signature encryption is used.
- The same MessageProtectionOrder is used to sign then encrypt the Message Service Request and Response.

Below you find links to the SOAP request and response:

Signature Confirmation with Encrypted Signature Request
Signature Confirmation with Encrypted Signature Response

7 Out of Scope

The primary objective for the MessageService scenarios is to demonstrate interoperability of Web services secured using WS-Security (WSS 1.1) and the Basic Security Profile version 1.1. For this reason, some requirements that would normally be considered in developing an application for deployment in a production environment have been ruled as out of scope.

Appendix A - Document References

Table 3: Documents of interest to this BSP 1.1 scenarios

Ref	Document	Description
SCMSA	SCM Security Architecture	The SCM Security Architecture document version 5.0.
BSP11	Basic Security Profile 1.1	The Basic Security Profile 1.1 provides guidance on the use of WS-Security 1.1 and the REL, Kerberos, SAML, UserName and X.509 security token formats.
BSP10	Basic Security Profile Version 1.0	A set of non-proprietary Web services specifications, along with clarifications to and amplifications of those specifications which promote interoperability
SCTC	Security Challenges Threats and Countermeasures	Identifies security challenges and the typical threats that prevent accomplishment of each challenge. Identifies the typical countermeasures (technologies and protocols) used to mitigate each threat
WSS10	Web Services Security Version 1.0	Delivers a technical foundation for implementing security functions such as integrity and confidentiality in messages implementing higher-level Web services applications
WSS11	Web Services Security Version 1.1	Describes additional or enhanced capabilities that build on those enabled or developed in WSS 1.0.

Appendix B – X.509 Certificate Summary

The following table contains the filenames of the Keys and Certificates required to exercise the BSP 1.1 MessageService scenarios.

Table 4: Keys and Certificates required used by MessageService scenarios

Keys and Certificates	Filename
Certifying CA certificate	**myca.cer**
MessageService Service private key	**bob-key.p12**
MessageService Service certificate	**bob-cert.der**
MessageService Client private Key	**alice-key.p12**
MessageService Client certificate	**alice-cert.der**

The following table contains the *MessageService Service-side configuration.*

A third-party is expected to provide its own keys and certificates for testing BSP 1.1. These keys are not provided in the scenario package.

Table 5: MessageService Service-side configuration.

Service provider(service-side)			
	Operation	**Alias**	**DN**
Request Inbound	Signature Verification	myca	CN=myca, OU=sec, O=ca3
	Decryption	bob	CN=bob, OU=myou, O=myco
Response Outbound	**Operation**	**Alias**	**DN**
	Signing	bob	CN=bob, OU=myou, O=myco
	Encryption	alice	CN=alice, OU=myou, O=myco

The following table contains the *MessageService client-side configuration.*

Table 6: MessageService Client-side configuration.

Service consumer (client-side)			
Request Outbound	**Operation**	**Alias**	**DN**
	Signing	alice	CN=alice, OU=myou, O=myco
	Encryption	bob	CN=bob, OU=myou, O=myco
Response Inbound	**Operation**	**Alias**	**DN**
	Signature Verification	myca	CN=myca, OU=sec, O=ca3
	Decryption	alice	CN=alice, OU=myou, O=myco

The certificate chain below explains the relationships between the certificates:

The myca certificate is self-signed by the myca test Certificate Authority (CA).

All other certificates are signed by the myca CA.

Note that different certificates are used for signing and encrypting messages.

Appendix C – MessagesService wsdl

Figure 1: MessageService wsdl

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions name="getMessage"
    targetNamespace="http://www.example.org/getMessage/"
    xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
    xmlns:tns="http://www.example.org/getMessage/"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
    <wsdl:types>
        <xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            targetNamespace="http://www.example.org/getMessage/">
            <xsd:element name="getMessageOperationElementReq">
                <xsd:complexType>
                    <xsd:sequence>
                        <xsd:element name="getMessageOutput"
                            type="xsd:string">
                        </xsd:element>
                    </xsd:sequence>
                </xsd:complexType>
            </xsd:element>
            <xsd:element name="getMessageOperationElementResp">
                <xsd:complexType>
                    <xsd:sequence>
                        <xsd:element name="getMessageInput"
                            type="xsd:string">
                        </xsd:element>
                    </xsd:sequence>
                </xsd:complexType>
            </xsd:element>
            <xsd:element name="msgHeaderElement">
                <xsd:complexType>
                    <xsd:sequence>
                        <xsd:element name="msgHeaderInput"
                            type="xsd:string">
                        </xsd:element>
                    </xsd:sequence>
                </xsd:complexType>
            </xsd:element>
        </xsd:schema>
    </wsdl:types>
    <wsdl:message name="getMessageOperationRequest">
        <wsdl:part name="inputPart"
            element="tns:getMessageOperationElementReq">
        </wsdl:part>
        <wsdl:part name="msgReqHeaderPart"
            element="tns:msgHeaderElement">
        </wsdl:part>
    </wsdl:message>
    <wsdl:message name="getMessageOperationResponse">
        <wsdl:part name="outPart"
            element="tns:getMessageOperationElementResp">
        </wsdl:part>
    </wsdl:message>
    <wsdl:portType name="getMessagePortType">
        <wsdl:operation name="getMessageOperation">
            <wsdl:input message="tns:getMessageOperationRequest"></wsdl:input>
            <wsdl:output message="tns:getMessageOperationResponse"></wsdl:output>
        </wsdl:operation>
    </wsdl:portType>
    <wsdl:binding name="getMessageBinding"
        type="tns:getMessagePortType">
        <soap:binding style="document"
            transport="http://schemas.xmlsoap.org/soap/http" />
        <wsdl:operation name="getMessageOperation">
            <soap:operation
                soapAction="http://www.example.org/getMessage/getMessageOperation" />
            <wsdl:input>
                <soap:body use="literal" parts="inputPart" />
                <soap:header message="tns:getMessageOperationRequest"
                    part="msgReqHeaderPart" use="literal" wsdl:required="true">
                </soap:header>
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal" />
            </wsdl:output>
        </wsdl:operation>
    </wsdl:binding>
    <wsdl:service name="MessageService">
        <wsdl:port name="getMessagePort"
            binding="tns:getMessageBinding">
            <soap:address
                location="http://localhost:9080/MessageService/getMessage">
            </soap:address>
        </wsdl:port>
    </wsdl:service>
</wsdl:definitions>
```

Appendix D – SOAP Messages Examples

This section contains examples of secured and unsecured SOAP request and response messages for the following messages:

MessageService Request with no QoS applied

MessageService Response with no QoS applied

MessageService Request with Encrypted SOAP Header Feature (wsu:Id for EncryptedHeader element)

MessageService Response with Encrypted SOAP Header Feature, (wsu:Id for EncryptedHeader element)

MessageService Request with Encrypted SOAP Header Feature

MessageService Response with Encrypted SOAP Header Feature

MessageService Request with Signature Confirmation Feature

MessageService Response with Signature Confirmation Feature

MessageService Request with Thumbprint Reference Feature

MessageService Response with Thumbprint Reference Feature

MessageService Request with Signature Confirmation Feature, Encrypted Signature [optional scenario]

MessageService Response with Signature Confirmation Feature, Encrypted Signature [optional scenario]

Figure 2: MessageService request with no QoS

Request call to MessageService. Request includes a Header Element in the clear.
This is the base scenario for Scenarios 1, 2, and 3.

```
<!--********************************************************************************
        POST /MessageService/MessageService HTTP/1.1
        Host: 127.0.0.1:9088
        Accept: application/soap+xml,multipart/related,text/*
        User-Agent: IBM WebServices/1.0
        Cache-Control: no-cache
        Pragma: no-cache
        SOAPAction: "http://www.example.org/getMessage/getMessageOperation"
        Connection: Keep-Alive
        Content-Type: text/xml; charset=UTF-8
        Content-Length: 507
        Date: Fri, 07 Mar 2008 03:24:21 GMT
    -->
    <?xml version="1.0" encoding="UTF-8"?>
    <soapenv:Envelope
        xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
        <soapenv:Header>
            <ns2:msgHeaderElement
                xmlns:ns2="http://www.example.org/getMessage/">
                <msgHeaderInput>Header of Request</msgHeaderInput>
            </ns2:msgHeaderElement>
        </soapenv:Header>
        <soapenv:Body>
            <ns2:getMessageOperationElementReq
                xmlns:ns2="http://www.example.org/getMessage/">
                <getMessageOutput>BODY OF Request</getMessageOutput>
            </ns2:getMessageOperationElementReq>
        </soapenv:Body>
    </soapenv:Envelope>
```

Figure 3: MessagesService response with no QoS

Response of MessageService. This is base scenario for Scenarios 1, 2, and 3.

```
<!--*********************************************************************************

                        HTTP/1.1 200 OK
                        Content-Type: text/xml; charset=UTF-8
                        Content-Language: en-US
                        Content-Length: 387
                        Date: Fri, 07 Mar 2008 03:24:20 GMT
                        Server: WebSphere Application Server/6.1
            -->

            <?xml version="1.0" encoding="UTF-8"?>
            <soapenv:Envelope
                        xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
                        <soapenv:Body>
                                    <ns2:getMessageOperationElementResp
                                                xmlns:ns2="http://www.example.org/getMessage/">
                                                <getMessageInput>
                                                            Service &gt;&gt; Header: Header of Request and Body:
                                                            Header of Request
                                                </getMessageInput>
                                    </ns2:getMessageOperationElementResp>
                        </soapenv:Body>
            </soapenv:Envelope>
```

Figure 4: Encrypted SOAP Header scenario Message Service request (wsu:Id for EncryptedHeader element)

Scenario 1: Encrypted SOAP Header (wsu:Id for EncryptedHeader element) with Basic128Rsa15 Algorithms Suite.

```
<!--*********************************************************************************
                Scenario 1: Encrypted SOAP Header (wsu:Id for EncryptedHeader element) with Basic128Rsa15 Algorithms Suite
                Exercises the Encrypted Header requirements.
                Message Service Request encrypts the Header Element (SOAP message header) and then the Body.
                Request signs Timestamp, Body and the Header Element.
                The encrypted ReferenceList uses the wsu:Id of the EncryptedHeader element to reference the encryption.
                No signature encryption is used.
                The same MessageProtectionOrder is used to encrypt and then sign the Message Service Request and Response.
                ****************************************************************************************
                                HTTP/1.1 200 OK
                                Content-Type: text/xml; charset=UTF-8
                                Content-Language: en-US
                                Content-Length: 6637
                                Date  Mon, 14 Sep 2009 19:35:29 GMT
-->

<?xml version="1.0" encoding="UTF-8"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd">
  <s:Header>
   <k:EncryptedHeader s:mustUnderstand="1" u:Id="_3" xmlns:k="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd">
    <e:EncryptedData xmlns:e="http://www.w3.org/2001/04/xmlenc#">
     <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"></e:EncryptionMethod>
     <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
      <o:SecurityTokenReference k:TokenType="http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey" xmlns:o="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
       <o:Reference ValueType="http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey" URI="#_0"></o:Reference>
      </o:SecurityTokenReference>
     </KeyInfo>
     <e:CipherData>

<e:CipherValue>2lOb6lLLQqHHVOdA2v0sfrw853K4yi008SWrOxOUy7MPt78fNXRY1fOX3K3BHlYidXUMBLstWoZLQ3uXJy7FohzMo5YkY8E6q0yGEW7yPOfBUHWcuU1a7
8sLvDAxxJ1UJrgwlmWxx27ehhj2Bs5wlWovb54CB6kv+EW5nsYxny7koQfNnGtrLY3pseQjjGBorl4ABoKuuogWIgjBOJrzLdrKeL+9zi7TSL+aEFOAG+OVE3jGuCsM9/oCjf3j5Xx
i0mLM4cG7lipXVwSzhUwZBnLy5vnxTkuwq2rGlNJF/kmxsSKXYCwYF6A1zoxm6ah8ppHNH9hLnPEZsJNykyr2jxhGImHvTDZhz7PTxA4upUY=</e:CipherValue>
     </e:CipherData>
    </e:EncryptedData>
   </k:EncryptedHeader>
   <o:Security s:mustUnderstand="1" xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
    <u:Timestamp u:Id="uuid-f9bcec3b-d47c-4598-aff7-c3cef2c78934-1">
     <u:Created>2009-09-14T19:35:33.204Z</u:Created>
     <u:Expires>2009-09-14T19:40:33.204Z</u:Expires>
    </u:Timestamp>
    <o:BinarySecurityToken>
     <!-- Removed-->
    </o:BinarySecurityToken>
    <e:EncryptedKey Id="_0" xmlns:e="http://www.w3.org/2001/04/xmlenc#">
     <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"></e:EncryptionMethod>
     <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
      <o:SecurityTokenReference>
       <o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509SubjectKeyIdentifier"
EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-
1.0#Base64Binary">e3PQ5RxqF7scgTwXw/AwvrQ3fdQ=</o:KeyIdentifier>
      </o:SecurityTokenReference>
     </KeyInfo>
     <e:CipherData>

<e:CipherValue>C6qymVIeaZPcigd4yYvWG3C06fHhBwSj+HBlc+KgwqxbeBuSTUKn4RTb+lcoTB33rVLZZxyQkMy7uUAMnNVVTtsVj30QYRamyo6ApnqLOb8CDm6Z+T9A6
B3IwlO1U5AMm5nNXaH5B5c85LNWbUf+Hs2sAix3PH+qAnbk29q5JBo=</e:CipherValue>
     </e:CipherData>
    </e:EncryptedKey>
```

```xml
      <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
        <SignedInfo>
          <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></CanonicalizationMethod>
          <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"></SignatureMethod>
          <Reference URI="#_2">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>WS9w+a1cj/BUs7WPeU/DDijDt8E=</DigestValue>
          </Reference>
          <Reference URI="#_3">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>FOBYep1zfC4i8rq6xgmLx2KSMQw=</DigestValue>
          </Reference>
          <Reference URI="#uuid-f9bcec3b-d47c-4598-aff7-c3cef2c78934-1">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>O9SIFVp8LiCe2CGRxTmkTwoj9LE=</DigestValue>
          </Reference>
        </SignedInfo>

<SignatureValue>YWoXbu8Ndgu9IXVkeVT0M5XOaKeh9NCzHm7tNrxJ/hNrvjXS1chD3RGE21VFCvmfme2oL3q5ZlzUp900eWl2pKBUWtPdXLTlcOVo+BqTM/EPEhdF+eaBI
6oErz9h+1wUh5mGl8WLnXQdyMum4v6P09i3Bn9vCe9Q8yobFOkrARU=</SignatureValue>
        <KeyInfo>
          <o:SecurityTokenReference>
            <o:Reference ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" URI="#uuid-39856a06-f07a-4aed-af5c-
8b93e7f4b3fb-2"></o:Reference>
          </o:SecurityTokenReference>
        </KeyInfo>
      </Signature>
      <e:ReferenceList xmlns:e="http://www.w3.org/2001/04/xmlenc#">
        <e:DataReference URI="#_1"></e:DataReference>
        <e:DataReference URI="#_3"></e:DataReference>
      </e:ReferenceList>
    </o:Security>
    <To s:mustUnderstand="1"
xmlns="http://schemas.microsoft.com/ws/2005/05/addressing/none">http://127.0.0.1/Security_BSP11_Service_WCF/Scenario1.svc</To>
    <Action s:mustUnderstand="1"
xmlns="http://schemas.microsoft.com/ws/2005/05/addressing/none">http://www.example.org/getMessage/getMessageOperation</Action>
  </s:Header>
  <s:Body u:Id="_2" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <e:EncryptedData Id="_1" Type="http://www.w3.org/2001/04/xmlenc#Content" xmlns:e="http://www.w3.org/2001/04/xmlenc#">
      <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"></e:EncryptionMethod>
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <o:SecurityTokenReference k:TokenType="http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey" xmlns:o="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:k="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd">
          <o:Reference ValueType="http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey" URI="#_0"></o:Reference>
        </o:SecurityTokenReference>
      </KeyInfo>
      <e:CipherData>

<e:CipherValue>+YDO7rf21YYXTgogsc5cPFJai0tHynSNkIpPRtZgJDTzQXwotPUm8r84ktuNc29a6WlzgIaFscbtv+JYWBEw8ujK8x+W8LWpFbUMfEJsag/YpoXPcPpIvPjXPFUp
GtdN+oCVQKOFQE5wbDn31Zqnf0REZNPQ8hD17qmwHMOGLYqIS33tY5XEd9Q4ztx/G+kmCvSPbI8Hw/lJAawEgBnL+m6S00EmHF0J5MQA/nAszxM3mpX08CV1Ui2WmZ
rI5IAQ9qHLeZfiZRC7WtY8wFi9guDsOy/ughpwWjOPzxelL7mcDmlbgFJLZ2hHHPRcAFgh8TZqajbEXcaxDjbnUfX2m2ykhoqnudaK4a6U4y4fpWs0LziJSNYm1e/OhahwozyD5
oWA9hUWNMM+2jF+xGhslg==</e:CipherValue>
      </e:CipherData>
    </e:EncryptedData>
  </s:Body>
</s:Envelope>
```

Figure 5: Encrypted SOAP Header scenario Message Service response (wsu:Id for EncryptedHeader element)

Scenario 1: Encrypted SOAP Header (wsu:Id for EncryptedHeader element) with Basic128Rsa15 Algorithms Suite.

```
<!--***************************************************************************************
          Scenario 1: Encrypted SOAP Header (wsu:Id for EncryptedHeader element) with Basic128Rsa15 Algorithms Suite
          Message Service Response encrypts the Body and signs Timestamp and Body.
          No signature encryption is used.
          The same MessageProtectionOrder is used to encrypt and then sign the Message Service Request and Response.
          **************************************************************************************************************
                    SOAPAction: "  http://www.example.org/getMessage/getEncHeaderPortType/getMessageOperationResponse"
                    Connection: Keep-Alive
                    Content-Type: text/xml; charset=UTF-8
                    Content-Length: 5322
                    Date: Mon, 14 Sep 2009 19:35:36 GMT
                    Server: Microsoft-IIS/7.5
-->
<?xml version="1.0" encoding="UTF-8"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd">
  <s:Header>
   <o:Security s:mustUnderstand="1" xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
    <u:Timestamp u:Id="uuid-201b9bb1-5375-4f90-9ece-e843547e88b6-5">
     <u:Created>2009-09-14T19:35:36.564Z</u:Created>
     <u:Expires>2009-09-14T19:40:36.564Z</u:Expires>
    </u:Timestamp>
    <o:BinarySecurityToken>
     <!-- Removed-->
    </o:BinarySecurityToken>
    <e:EncryptedKey Id="_0" xmlns:e="http://www.w3.org/2001/04/xmlenc#">
     <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"></e:EncryptionMethod>
     <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
      <o:SecurityTokenReference>
       <o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509SubjectKeyIdentifier"
EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-
1.0#Base64Binary">5g/R2lazG391d8Mugsmn7beQceg=</o:KeyIdentifier>
      </o:SecurityTokenReference>
     </KeyInfo>
     <e:CipherData>

<e:CipherValue>Ttjon55X3AKIUt71nhkXJcJ8L1JehBVy1btViROZWpdmL91qfdX7jmcCpYsUK5coVQPIc2q57FP3PgaqKNxHHaVaWfqOW9/oebiZ3x5k7iSI5/j8v/TEIdmfwgs
hHbI09tuOCz94LcZgLgs9ZRgrYZabXfw8KjdilnHxdfZwWus=</e:CipherValue>
     </e:CipherData>
    </e:EncryptedKey>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
     <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></CanonicalizationMethod>
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"></SignatureMethod>
      <Reference URI="#_2">
       <Transforms>
        <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
       </Transforms>
       <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
       <DigestValue>eAAHGCHZfRuOs4JdBZtXKiBA61Q=</DigestValue>
      </Reference>
      <Reference URI="#uuid-201b9bb1-5375-4f90-9ece-e843547e88b6-5">
       <Transforms>
        <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
       </Transforms>
       <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
       <DigestValue>N2KswcVwtyppoekNDHg28btwOlA=</DigestValue>
      </Reference>
     </SignedInfo>
```

```
<SignatureValue>VD92WGvK4k1IMjVP3BIKlhqcpz7P5FE8gipB4HMR1Q4rEDTP8JqEFLflpwwbv4SyjEsVv0zZYpX/bF6I4dNJoKykUUuBboWn/XJ47zrM9og2eMIEly9FBUEjD
BlYpFZowvMErKcibwp9iYVB22wlHKK0kqpVgTuq0ySKPzMb6kc=</SignatureValue>
     <KeyInfo>
      <o:SecurityTokenReference>
       <o:Reference ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" URI="#uuid-fe8fa075-c45e-44c3-85e4-
4bd1672279a4-2"></o:Reference>
      </o:SecurityTokenReference>
     </KeyInfo>
    </Signature>
    <e:ReferenceList xmlns:e="http://www.w3.org/2001/04/xmlenc#">
     <e:DataReference URI="#_1"></e:DataReference>
    </e:ReferenceList>
   </o:Security>
  </s:Header>
  <s:Body u:Id="_2" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
   <e:EncryptedData Id="_1" Type="http://www.w3.org/2001/04/xmlenc#Content" xmlns:e="http://www.w3.org/2001/04/xmlenc#">
    <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"></e:EncryptionMethod>
    <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
     <o:SecurityTokenReference k:TokenType="http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey" xmlns:o="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:k="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd">
      <o:Reference ValueType="http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey" URI="#_0"></o:Reference>
     </o:SecurityTokenReference>
    </KeyInfo>
    <e:CipherData>

<e:CipherValue>8wym0i6ftjkWFlHGTNJKjoDw39l2aQt4ykAV0A97eIXXdvhgNtAqDOPIa1QqXP+rZFbr4aFSSdWWm1hUns9flqN4lYu5CBqBjSRnZ0rEzqiqw2t5K9YAATebFk
HFgQy5H4S99iYaWcdYDAkyvyPKKFANYVRfLLBjw9MCVXFUJwbjkqFeZEotDKKgYSk+rA8ESdOirjv9jtGzCDWxYETlj6YNbNlqhScNkjkEfIwshVxmR1+ONW2hC6U4NJAt9LCfK
v973vk5uFCRwVmUrGoDgf1C7mTEcuIFrOFaSHbOTI5TPEipmdbYwqO36SYmE+ovYGk9Fek8mlYL+cBFm+eGL8qJkgo12l2/0+aaUBT05WwkbXAfxzAEzpysb+nqPxFhEHhN
mDFzzHdR3O9EV7D7VPZzOo2s56v9+5+v7RUfm3FcbxXO2gF6mVoVOcfu0UpLSkZ/EgentUr/uihIdM2IZGQT3oDY9VuLzkaRf5nkb9pwa6Jdi+JIFUaOOuK9iKvp</e:CipherV
alue>
    </e:CipherData>
   </e:EncryptedData>
  </s:Body>
 </s:Envelope>
```

Figure 6: Encrypted SOAP Header scenario Message Service request

Scenario 1: Encrypted SOAP Header with Basic128Rsa15 Algorithms Suite.

```
<!--*************************************************************************************
    Scenario 1: Encrypted Header with Basic128Rsa15 Algorithms Suite
    Exercises the Encrypted Header and Encrypted Data contained in an Encrypted Header requirements.
    Message Service Request encrypts the Header Element (SOAP message header) and then the Body.
    Request signs Timestamp, Body and the Header Element.
    The encrypted ReferenceList uses the EncryptedData id within the EncryptedHeader element to reference the encryption.
    No signature encryption is used.
    The same MessageProtectionOrder is used to encrypt and then sign the Message Service Request and Response.
    ****************************************************************************************************


        POST /MessageService/MessageService HTTP/1.1
        Host: 127.0.0.1:9088
        Accept: application/soap+xml,multipart/related,text/*
        User-Agent: IBM WebServices/1.0
        Cache-Control: no-cache
        Pragma: no-cache
        SOAPAction: "http://www.example.org/getMessage/getMessageOperation"
        Connection: Keep-Alive
        SAVECONNECTION: 18360845921238523266046
        IBM-WAS-CLIENT: TRUE
        Content-Type: text/xml; charset=UTF-8
        Content-Length: 5330
        Date: Tue, 31 Mar 2009 18:14:25 GMT
    →

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
    <soapenv:Header>
        <wsse:Security
            xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
            soapenv:mustUnderstand="1">
            <wsu:Timestamp
                xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
                wsu:Id="wssecurity_signature_id_22">
                <wsu:Created>2009-05-27T03:07:47.125Z
                </wsu:Created>
                <wsu:Expires>2009-05-27T03:12:47.156Z
                </wsu:Expires>
            </wsu:Timestamp>
            <wsse:BinarySecurityToken
                xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
                wsu:Id="x509bst_26"
                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">

    MIICSjCCAbOgAwIBAgIBEjANBgkqhkiG9w0BAQUFADArMQwwCgYDVQQKEwNjYTMxDDAKBgNVBAsTA3NlYzENMAsGA1UEAxMEbXljYTAeFw0wODA5MTYxN
TI0NTVaFw0xMTA2MTMxNTI0NTVaMC4xDTALBgNVBAoTBG15Y28xDTALBgNVBAsTBG15b3UxDjAMBgNVBAMTBWFsaWNlMIGfMA0GCSqGSIb3DQEBAQUAA4GNADC
BiQKBgQDeSazc2OxPpmHgOJJYsIUar6sEEfOzVuYCwhTzPo3OKBUotwWvoH87j27FU863i0rpm6mE1COvPfgsfLxv/5j9MBA57zAisKwGTjKjDCmUGHr6zjpvPIDWzBgRW5qg
y+73rVjM4Q9jdYJ8SYu8Bcsok2D7v2kqAf4keJricK4PnQIDAQABo3sweTAJBgNVHRMEAjAAMCwGCWCGSAGG+EIBDQQfFh1PcGVuU1NMIEdlbmVyYXRlZCBDZXJ0aWZpY2
F0ZTAdBgNVHQ4EFgQU5g/R2lazG391d8Mugsmn7beQcegwHwYDVR0jBBgwFoAUAQB/1l88r1HCu3ZR4OZo3uw/QeowDQYJKoZIhvcNAQEFBQADgYEAmkOAUMpqqCqc
jusQ4GFdRcBev2sH5VHV59+gDbrJz74LozQHlYWhx/Ib32i3Ff6bQ2Lr8+4h0TyT3Sv5qaOA5aTPaklu2e9sS6NM1XvTa7c4Hfb+7c9vqG0JB/J78t8Vg5ZPHsIdEEZxRqA6VrpAH
8FOldacey4w7i5zyBytQgE=
            </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#">
                        <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
                            PrefixList="soapenv wsse ds "></ec:InclusiveNamespaces>
                    </ds:CanonicalizationMethod>
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"></ds:SignatureMethod>
                    <ds:Reference URI="#wssecurity_signature_id_22">
```

```
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                <ec:InclusiveNamespaces
                                    xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="soapenv wsu wsse "></ec:InclusiveNamespaces>
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod>
                        <ds:DigestValue>6Pu+ayS+ETolCJhgP7UeiWw6b9g=
                        </ds:DigestValue>
                    </ds:Reference>
                    <ds:Reference URI="#wssecurity_signature_id_23">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                <ec:InclusiveNamespaces
                                    xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="soapenv wsu enc wsse11 "></ec:InclusiveNamespaces>
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod>
                        <ds:DigestValue>tikGhcP8ZdOD8UWtxZMxCLm/rvk=
                        </ds:DigestValue>
                    </ds:Reference>
                    <ds:Reference URI="#wssecurity_signature_id_24">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                <ec:InclusiveNamespaces
                                    xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="soapenv enc wsse ds "></ec:InclusiveNamespaces>
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod>
                        <ds:DigestValue>NnvFBFHDho7ykQuErdWhyiwXbAY=
                        </ds:DigestValue>
                    </ds:Reference>
                    <ds:Reference URI="#wssecurity_signature_id_25">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                <ec:InclusiveNamespaces
                                    xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="soapenv wsu enc "></ec:InclusiveNamespaces>
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod>
                        <ds:DigestValue>q0pNkgwYvuRu9HOfUed0gFyUVrw=
                        </ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>
                <ds:SignatureValue>

    d1y00zwyH3u2puwRO1F1nTFZPn5DbNlGBWrbQrffBcWBlTipMWbpV4+O43l8z0MKejc2EtfMbX1dxP1rY9YH+Y+oc7ejj+ZauyMJC4P5/thR13UYMAVItMhi4CG
oQFFmgFztPqZRCzYzKxiU0S+yjna1JDhfgw8tIaeyIRa9GNU=
                </ds:SignatureValue>
                <ds:KeyInfo>
                    <wsse:SecurityTokenReference>
                        <wsse:Reference URI="#x509bst_26"
                            ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-
profile-1.0#X509v3"></wsse:Reference>
                    </wsse:SecurityTokenReference>
                </ds:KeyInfo>
            </ds:Signature>
            <enc:EncryptedKey xmlns:enc="http://www.w3.org/2001/04/xmlenc#"
                Id="wssecurity_signature_id_24">
                <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"></enc:EncryptionMethod>
                <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                    <wsse:SecurityTokenReference>
```

```
                        <wsse:KeyIdentifier
                            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#X509SubjectKeyIdentifier">e3PQ5RxqF7scgTwXw/AwvrQ3fdQ=
                        </wsse:KeyIdentifier>
                    </wsse:SecurityTokenReference>
                </ds:KeyInfo>
                <enc:CipherData>
                    <enc:CipherValue>

    SVFV7vfPycm55EkAyjgT3LOPTNap8tBAU1ZGSft/x/wZ2YiamyxIZGcYl//8epaZgi8XmhOhe0ECir6/lBXgR7TGUDOCAHItZ+w3Q9dmYW3EhEcayT+X4nEU2dFS2z
xJfgbxQZ698VxlMPEVzcDcvh8sExjp4fY/MybcOu4CCTA=
                    </enc:CipherValue>
                </enc:CipherData>
                <enc:ReferenceList>
                    <enc:DataReference URI="#wssecurity_encryption_id_20"></enc:DataReference>
                    <enc:DataReference URI="#wssecurity_encryption_id_21"></enc:DataReference>
                </enc:ReferenceList>
            </enc:EncryptedKey>
        </wsse:Security>
        <wsse11:EncryptedHeader
            xmlns:wsse11="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd"
            xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
            soapenv:mustUnderstand="1" wsu:Id="wssecurity_signature_id_23">
            <enc:EncryptedData xmlns:enc="http://www.w3.org/2001/04/xmlenc#"
                Id="wssecurity_encryption_id_20">
                <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"></enc:EncryptionMethod>
                <enc:CipherData>
                    <enc:CipherValue>

    MKaXVPgagi51NNCxqa1awGN31MHjwtBmvmab8NZ9loVkq21FFS48iflszNfOIlGFM6a/QCTsrSlkpla1eXJ/0S8AMAihwx4jY3layLJd6iqSInCCdI3Kz9cghYLD8A0M
fOrcXT5HA2wvENsbqUJy8nnt5jNW9xiKRjje+sUH99qry4pmX09kJa6yr+Gl4TR6ut05Oab/b4rwLeymEXQN5F48dm+ltmHhlx8hQs2/plE=
                    </enc:CipherValue>
                </enc:CipherData>
            </enc:EncryptedData>
        </wsse11:EncryptedHeader>
    </soapenv:Header>
    <soapenv:Body
        xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
        wsu:Id="wssecurity_signature_id_25">
        <enc:EncryptedData xmlns:enc="http://www.w3.org/2001/04/xmlenc#"
            Id="wssecurity_encryption_id_21" Type="http://www.w3.org/2001/04/xmlenc#Content">
            <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"></enc:EncryptionMethod>
            <enc:CipherData>
                <enc:CipherValue>

    Jy3M4dSA+u09rJsGxzSWW7clF3kpSZHXMHnaZLMKDYKtaF+QmXAtQ3LT+zm6ZrUqXjZ31CKWF8rWNWI6uZ4yG6syHe04kE5c5QUaTH8raHzKW1WKwZDiA70
hjdPCm3QYwFxCEzuL6hy6wMeknRAQHDqqMsJH5eO3xT4PXL6y7vxp2IveQlIGsg+gquzFBDGPCCuL1BEsZ23ipUSIuF+88R801La1Dh4s4ULzvGt9M20=
                </enc:CipherValue>
            </enc:CipherData>
        </enc:EncryptedData>
    </soapenv:Body>
</soapenv:Envelope>
```

Figure 7: Encrypted SOAP Header scenario Message Service response

Scenario 1: Encrypted SOAP Header with Basic128Rsa15 Algorithms Suite.

```
<!--*************************************************************
    Scenario 1: Encrypted SOAP Header with Basic128Rsa15 Algorithms Suite
    Message Service Response encrypts the Body and signs Timestamp and Body.
    No signature encryption is used.
    The same MessageProtectionOrder is used to encrypt and then sign the Message Service Request and Response.
    ****************************************************************************************************

        HTTP/1.1 200 OK
        Content-Type: text/xml; charset=UTF-8
        Content-Language: en-US
        Content-Length: 4756
        Date: Tue, 31 Mar 2009 18:14:25 GMT
        Server: WebSphere Application Server/7.0
    -->


<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
    <soapenv:Header>
        <wsse:Security
            xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
            soapenv:mustUnderstand="1">
            <wsu:Timestamp
                xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
                wsu:Id="wssecurity_signature_id_23">
                <wsu:Created>2009-05-27T03:07:50.843Z
                </wsu:Created>
                <wsu:Expires>2009-05-27T03:12:50.843Z
                </wsu:Expires>
            </wsu:Timestamp>
            <wsse:BinarySecurityToken
                xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
                wsu:Id="x509bst_24"
                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">

    MIICSDCCAbGgAwIBAgIBEzANBgkqhkiG9w0BAQUFADArMQwwCgYDVQQKEwNjYTMxDDAKBgNVBAsTA3NlYzENMAsGA1UEAxMEbXljYTAeFw0wODA5MTYx
NTI5NTdaFw0xMTA2MTMxNTI5NTdaMCwxDTALBgNVBAoTBG15Y28xDTALBgNVBAsTBG15b3UxDDAKBgNVBAMTA2JvYjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCg
YEAmJSMY3x7aFeiyEaiv22VSKrg5Cj0djPxtoDTqKF2fXawVKF+M2e7PvPyGPeZYqWKG29FiEs0oeL+Mk3Bvu5OEj2ED2srG7KLbae6cDkhV05erkRoIuooaszztv9rEvJ9PQ3W1
SvajHa5njxx7EqhEFQLhjVdQN272jrS+jyTAIcCAwEAAaN7MHkwCQYDVR0TBAIwADAsBglghkgBhvhCAQ0EHxYdT3BlblNTTCBHZW5lcmF0ZWQgQ2VydGlmaWNhdGUwHQ
YDVR0OBBYEFHtz0OUcahe7HIE8F8PwML60N33UMB8GA1UdIwQYMBaAFAEAf9ZfPK9Rwrt2UeDmaN7sP0HqMA0GCSqGSIb3DQEBBQUAA4GBAJUgE9tOGHNpWrCxIZA
+SKLGhF8dmB3Tk08/l8NHPAXC7ZJR4RpaBq7mQM+D5o/Qmn2KneBb0F8fQa4HeG15hg4flk1f2544brkt/8XUVPSG/rAjXG0kIvcAZhj7Ok56JUywbbLt4q3I02IUQkhZ+3wtI
2Xif4c2tHYbSZk5G2Ii
            </wsse:BinarySecurityToken>
            <wsse11:SignatureConfirmation
                xmlns:wsse11="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd"
                xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"

    Value="d1y00zwyH3u2puwRO1F1nTFZPn5DbNlGBWrbQrffBcWBlTipMWbpV4+O43l8z0MKejc2EtfMbX1dxP1rY9YH+Y+oc7ejj+ZauyMJC4P5/thR13UYMAVIt
Mhi4CGoQFFmgFztPqZRCzYzKxiU0S+yjna1JDhfgw8tIaeyIRa9GNU="
                wsu:Id="wssecurity_sigconf_id_20"></wsse11:SignatureConfirmation>
            <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#">
                        <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
                            PrefixList="soapenv wsse ds "></ec:InclusiveNamespaces>
                    </ds:CanonicalizationMethod>
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"></ds:SignatureMethod>
                    <ds:Reference URI="#wssecurity_signature_id_22">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                <ec:InclusiveNamespaces
                                    xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="soapenv wsu enc "></ec:InclusiveNamespaces>
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod>
                        <ds:DigestValue>2XkimHx0yWsUzxbBwjsuGRZ62pU=
                        </ds:DigestValue>
                    </ds:Reference>
                    <ds:Reference URI="#wssecurity_sigconf_id_20">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                <ec:InclusiveNamespaces
                                    xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="soapenv wsu wsse wsse11 "></ec:InclusiveNamespaces>
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod>
                        <ds:DigestValue>HMhKooMfBhsgNqOiYNi/yvqByKY=
                        </ds:DigestValue>
                    </ds:Reference>
                    <ds:Reference URI="#wssecurity_signature_id_23">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                <ec:InclusiveNamespaces
                                    xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="soapenv wsu wsse "></ec:InclusiveNamespaces>
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod>
                        <ds:DigestValue>420vZSGHWDAFGi+ywMSeeXiyUFM=
                        </ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>
                <ds:SignatureValue>

    NO7K6chzBo/kQel/VxLHUTvkST+MOJs19zHFkwByBTpQJfe/oHjkS+TS0wp9lAGGCjWNaRP1VpYKeTbMyhAgCsHXelUQEkIfhpSx4EAt45d93Cy9tRSlvKtZ4KGf5
mnGXAiDU+dnqGtoPRUgK0BKZ67GllCeueuClDKa8acSBFs=
                </ds:SignatureValue>
                <ds:KeyInfo>
                    <wsse:SecurityTokenReference>
                        <wsse:Reference URI="#x509bst_24"
                            ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-
profile-1.0#X509v3"></wsse:Reference>
                    </wsse:SecurityTokenReference>
                </ds:KeyInfo>
            </ds:Signature>
            <enc:EncryptedKey xmlns:enc="http://www.w3.org/2001/04/xmlenc#">
                <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"></enc:EncryptionMethod>
                <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                    <wsse:SecurityTokenReference>
                        <wsse:KeyIdentifier
                            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#X509SubjectKeyIdentifier">5g/R2lazG391d8Mugsmn7beQceg=
                        </wsse:KeyIdentifier>
                    </wsse:SecurityTokenReference>
                </ds:KeyInfo>
                <enc:CipherData>
                    <enc:CipherValue>
```

```
        aDWUjqGI3OBtfWLnEcYi75yslpXFoFpPyP1SkFjas0mG3sUr5B7BP4ISt5A/obBzworpWycGWktQd9R2te8sM7IxQsFaRgHKDT/WiMxEAM+k3lNpStHrupgtKwYPj
yiWcVmQygPm1WjmudgnAvS+gW2Uu59UEca4WrvbwYZorDM=
                                        </enc:CipherValue>
                                </enc:CipherData>
                                <enc:ReferenceList>
                                        <enc:DataReference URI="#wssecurity_encryption_id_21"></enc:DataReference>
                                </enc:ReferenceList>
                        </enc:EncryptedKey>
                </wsse:Security>
        </soapenv:Header>
        <soapenv:Body
                xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
                wsu:Id="wssecurity_signature_id_22">
                <enc:EncryptedData xmlns:enc="http://www.w3.org/2001/04/xmlenc#"
                        Id="wssecurity_encryption_id_21" Type="http://www.w3.org/2001/04/xmlenc#Content">
                        <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"></enc:EncryptionMethod>
                        <enc:CipherData>
                                <enc:CipherValue>

        +USJQnscA3TBQoBXZx/7/nrmT8Q7bRA5yny4HtI2j+A1F/vK5bczNiVIcQ47kr8V1V9F21LVNlDGvA+q1WkW1tY35gKpcSRxITZvQGiOCU++fE3lw9X4CvEA5leLKSY
m2GbFp7KR7QeLJcx2unGOVHp2PE/0+u8yPMek3/uwqKxsdJ2x45qBf7Xk+4iHTOIqJwXzV99DPsz5WehVGaLc11TZtPrRLB00IEZp5QGtE2pTbrcb8jwvKXnYpRZc3oW53L2W
H1wP6lYTBmiTLd0Fsj+XelT0agVPWJjNvauOZxw=
                                </enc:CipherValue>
                        </enc:CipherData>
                </enc:EncryptedData>
        </soapenv:Body>
</soapenv:Envelope>
```

Figure 8: Signature Confirmation scenario Message Service request

Scenario 2: Signature Confirmation, see response. Algorithms Suite Basic128Rsa15.

```
<!--*********************************************************************************

                Scenario 2: Signature Confirmation, see response. Algorithms Suite Basic128Rsa15.
                Request below Signs Timestamp, Body and the Encrypts Body. No Signature Encryption
                Same MessageProtectionOrder for request and responses of sign then encrypt.
                ***********************

                POST /MessageService/MessageService HTTP/1.1
                Host: 127.0.0.1:9088
                Accept: application/soap+xml,multipart/related,text/*
                User-Agent: IBM WebServices/1.0
                Cache-Control: no-cache
                Pragma: no-cache
                SOAPAction: "http://www.example.org/getMessage/getMessageOperation"
                Connection: Keep-Alive
                SAVECONNECTION: 12828212381238524202453
                IBM-WAS-CLIENT: TRUE
                Content-Type: text/xml; charset=UTF-8
                Content-Length: 4850
                Date: Tue, 31 Mar 2009 18:30:02 GMT
        -->

        <soapenv:Envelope
                xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
                <soapenv:Header>
                        <s:Security
                                xmlns:s="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
                                xmlns:x="http://www.w3.org/2001/10/xml-exc-c14n#"
                                xmlns:d="http://www.w3.org/2000/09/xmldsig#"
                                xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
                                xmlns:e="http://www.w3.org/2001/04/xmlenc#"
                soapenv:mustUnderstand="1">
                <u:Timestamp u:Id="w_20">
                    <u:Created>2009-03-31T18:30:00.171Z</u:Created>
                    <u:Expires>2009-03-31T18:35:00.187Z</u:Expires>
                </u:Timestamp>
                <s:BinarySecurityToken
                    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"
                    u:Id="x509bst_22">

    MIICSjCCAbOgAwIBAgIBEjANBgkqhkiG9w0BAQUFADArMQwwCgYDVQQKEwNjYTMxDDAKBgNVBAsTA3NlYzENMAsGA1UEAxMEbXljYTAeFw0wODA5MTYxN
TI0NTVaFw0xMTA2MTMxNTI0NTVaMC4xDTALBgNVBAoTBG15Y28xDTALBgNVBAsTBG15b3UxDjAMBgNVBAMTBWFsaWNlMIGfMA0GCSqGSIb3DQEBAQUAA4GNADC
BiQKBgQDeSazc2OxPpmHgOJJYsIUar6sEEfOzVuYCwhTzPo3OKBUotwWvoH87j27FU863i0rpm6mE1COvPfgsfLxv/5j9MBA57zAisKwGTjKjDCmUGHr6zjpvPIDWzBgRW5qg
y+73rVjM4Q9jdYJ8SYu8Bcsok2D7v2kqAf4keJricK4PnQIDAQABo3sweTAJBgNVHRMEAjAAMCwGCWCGSAGG+EIBDQQfFh1PcGVuU1NMIEdlbmVyYXRlZCBDZXJ0aWZpY2
F0ZTAdBgNVHQ4EFgQU5g/R2lazG391d8Mugsmn7beQcegwHwYDVR0jBBgwFoAUAQB/1l88r1HCu3ZR4OZo3uw/QeowDQYJKoZIhvcNAQEFBQADgYEAmkOAUMpqqCqc
jusQ4GFdRcBev2sH5VHV59+gDbrJz74LozQHlYWhx/Ib32i3Ff6bQ2Lr8+4h0TyT3Sv5qaOA5aTPaklu2e9sS6NM1XvTa7c4Hfb+7c9vqG0JB/J78t8Vg5ZPHsIdEEZxRqA6VrpAH
8FOldacey4w7i5zyBytQgE=
                </s:BinarySecurityToken>
                <e:EncryptedKey>
                    <e:EncryptionMethod
                        Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5">
                    </e:EncryptionMethod>
                    <d:KeyInfo>
                        <s:SecurityTokenReference>
                            <s:KeyIdentifier
                                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#X509SubjectKeyIdentifier">
                                e3PQ5RxqF7scgTwXw/AwvrQ3fdQ=
                            </s:KeyIdentifier>
                        </s:SecurityTokenReference>
                    </d:KeyInfo>
                    <e:CipherData>
                        <e:CipherValue>

    bJwSYDhwLFmBXOfv1zDPdz+olagDMsgRKYhjMr9DuFVympbd2I+vGdDxP/G2DwQPIVqNZAqx4xmxu37pPiNApzihywozkCoDU2mUFM40eV8mi2Dc7kzuW4a+
eWO4U41uM3Z6DNIdq68W9/jCLQzwEdzowvhVIj5tGd1Gzd4a7Lw=
                        </e:CipherValue>
                    </e:CipherData>
                    <e:ReferenceList>
                        <e:DataReference URI="#w_23"></e:DataReference>
                    </e:ReferenceList>
                </e:EncryptedKey>
                <d:Signature>
                    <d:SignedInfo>
                        <d:CanonicalizationMethod
                            Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                            <x:InclusiveNamespaces
                                PrefixList="d s soapenv ">
                            </x:InclusiveNamespaces>
                        </d:CanonicalizationMethod>
                        <d:SignatureMethod
                            Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1">
                        </d:SignatureMethod>
                        <d:Reference URI="#w_20">
                            <d:Transforms>
                                <d:Transform
                                    Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                    <x:InclusiveNamespaces
                                        PrefixList="s soapenv u ">
                                    </x:InclusiveNamespaces>
                                </d:Transform>
                            </d:Transforms>
                            <d:DigestMethod
```

```
                                Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
                            </d:DigestMethod>
                            <d:DigestValue>
                                JpnSjY4+hMj+Gv8zJGDc3qteHms=
                            </d:DigestValue>
                        </d:Reference>
                        <d:Reference URI="#w_21">
                            <d:Transforms>
                                <d:Transform
                                    Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                    <x:InclusiveNamespaces
                                        PrefixList="soapenv wsu ns2 ">
                                    </x:InclusiveNamespaces>
                                </d:Transform>
                            </d:Transforms>
                            <d:DigestMethod
                                Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
                            </d:DigestMethod>
                            <d:DigestValue>
                                kr3Tfss5fKzdGaoQswFQW/3ChMk=
                            </d:DigestValue>
                        </d:Reference>
                    </d:SignedInfo>
                    <d:SignatureValue>

    UKeFf86T2VknyDZ66Oor21fx+diVq+T0b9jLbhhzt0RRzhYxuaVAS8U8VdmydlLHjT5COJG1JSP1w1EOv0tnid58HEunYKyFHIh2AVfnK5U6s02CrO9oN76bGgtt3CA
1BE672R/XkvHDaroYsmEUwNFNSEpeXaChWlcyDcys61M=
                    </d:SignatureValue>
                    <d:KeyInfo>
                        <s:SecurityTokenReference>
                            <s:Reference URI="#x509bst_22"
                                ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
x509-token-profile-1.0#X509v3">
                            </s:Reference>
                        </s:SecurityTokenReference>
                    </d:KeyInfo>
                </d:Signature>
            </s:Security>
            <ns2:msgHeaderElement
                xmlns:ns2="http://www.example.org/getMessage/">
                <msgHeaderInput>Header field of Request</msgHeaderInput>
            </ns2:msgHeaderElement>
        </soapenv:Header>
        <soapenv:Body
            xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
            wsu:Id="w_21">
            <e:EncryptedData xmlns:e="http://www.w3.org/2001/04/xmlenc#"
                Id="w_23" Type="http://www.w3.org/2001/04/xmlenc#Content">
                <e:EncryptionMethod
                    Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc">
                </e:EncryptionMethod>
                <e:CipherData>
                    <e:CipherValue>

    gwtOfVhw0wnOiDfmrHdlInk7EUq+s9IqiENWKDIBZy/ORhwVGJ00tCAcY2CBK4CY1iE7y7Va//ZOE3J7cReKulNSSQ30/Yha8l4b2pyk5UjjzgXQBwnIPJFmFrMYhk+
j8UySPk/Ct3OjXEAOu7P0cYrt9UN51qQAvuWGJizvmi63OksCpcP5kByPBKEKne8K/6tIpCGQgcjyQbfO/pL1/q5crDASCN9zl40tWl7slAJSO6RvFp5RyJsI6/WvEtEDOTOtR8JNh
etEzOIZhgaR7A==
                    </e:CipherValue>
                </e:CipherData>
            </e:EncryptedData>
        </soapenv:Body>
    </soapenv:Envelope>
```

Figure 9: Signature Confirmation scenario Message Service response

Scenario 2: Signature Confirmation.

```
<--**************************************************
    Scenario 2: Signature Confirmation.
        Response includes a Signed Signature Confirmation. The response also Signs Timestamp,
        Body, Signature Confirmation and Encrypts Body.  No Signature encryption
        ****************************************************************************************

        HTTP/1.1 200 OK
        Content-Type: text/xml; charset=UTF-8
        Content-Language: en-US
        Content-Length: 5486
        Date: Tue, 31 Mar 2009 18:30:03 GMT
        Server: WebSphere Application Server/7.0
    -->

    <?xml version="1.0" encoding="UTF-8"?>
    <soapenv:Envelope
        xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
        <soapenv:Header>
            <s:Security
                xmlns:s="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
                xmlns:x="http://www.w3.org/2001/10/xml-exc-c14n#"
                xmlns:t="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd"
                xmlns:d="http://www.w3.org/2000/09/xmldsig#"
                xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
                xmlns:e="http://www.w3.org/2001/04/xmlenc#"
                soapenv:mustUnderstand="1">
                <u:Timestamp u:Id="w_22">
                    <u:Created>2009-03-31T18:30:03.187Z</u:Created>
                    <u:Expires>2009-03-31T18:35:03.187Z</u:Expires>
                </u:Timestamp>
                <s:BinarySecurityToken
                    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"
                    u:Id="x509bst_23">

    MIICSDCCAbGgAwIBAgIBEzANBgkqhkiG9w0BAQUFADArMQwwCgYDVQQKEwNjYTMxDDAKBgNVBAsTA3NlYzENMAsGA1UEAxMEbXljYTAeFw0wODA5MTYx
NTI5NTdaFw0xMTA2MTMxNTI5NTdaMCwxDTALBgNVBAoTBG15Y28xDTALBgNVBAsTBG15b3UxDDAKBgNVBAMTA2JvYjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCg
YEAmJSMY3x7aFeiyEaiv22VSKrg5Cj0djPxtoDTqKF2fXawVKF+M2e7PvPyGPeZYqWKG29FiEs0oeL+Mk3Bvu5OEj2ED2srG7KLbae6cDkhV05erkRoIuooaszztv9rEvJ9PQ3W1
SvajHa5njxx7EqhEFQLhjVdQN272jrS+jyTAIcCAwEAAaN7MHkwCQYDVR0TBAIwADAsBglghkgBhvhCAQ0EHxYdT3BlblNTTCBHZW5lcmF0ZWQgQ2VydGlmaWNhdGUwHQ
YDVR0OBBYEFHtz0OUcahe7HIE8F8PwML60N33UMB8GA1UdIwQYMBaAFAEAf9ZfPK9Rwrt2UeDmaN7sP0HqMA0GCSqGSIb3DQEBBQUAA4GBAJUgE9tOGHNpWrCxIZA
+SKLGhF8dmB3Tk08/l8NHPAXC7ZJR4RpaBq7mQM+D5o/Qmn2KneBb0F8fQa4HeG15hg4flk1f2544brkt/8XUVPSG/rAjXG0kIvcAZhj7Ok56JUywbbLt4q3I02IUQkhZ+3wtI
2Xif4c2tHYbSZk5G2Ii
                </s:BinarySecurityToken>
                <t:SignatureConfirmation

    Value="UKeFf86T2VknyDZ66Oor21fx+diVq+T0b9jLbhhzt0RRzhYxuaVAS8U8VdmydlLHjT5COJG1JSP1w1EOv0tnid58HEunYKyFHIh2AVfnK5U6s02CrO9oN76b
Ggtt3CA1BE672R/XkvHDaroYsmEUwNFNSEpeXaChWlcyDcys61M="
                    u:Id="w_20">
                </t:SignatureConfirmation>
                <e:EncryptedKey>
                    <e:EncryptionMethod
                        Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5">
                    </e:EncryptionMethod>
                    <d:KeyInfo>
                        <s:SecurityTokenReference>
                            <s:KeyIdentifier
                                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#X509SubjectKeyIdentifier">
                                5g/R2lazG391d8Mugsmn7beQceg=
                            </s:KeyIdentifier>
                        </s:SecurityTokenReference>
                    </d:KeyInfo>
                    <e:CipherData>
                        <e:CipherValue>

    mJ+StsQHJrvaZHkAMYUHpC094tQcXgx4C3zfcCnhZ0pPu0MIDrsonAX9nmw99X4HOd6cMTUx3exsljBk4MSCXv+2txqORM+tXhOs3azRrngywuioF0XLIzpJ2586c
cgEghnH90GeaI7pbFArlzBeQrCVbDCyL4G+sESjIfwkygk=
                        </e:CipherValue>
                    </e:CipherData>
                    <e:ReferenceList>
                        <e:DataReference URI="#w_24"></e:DataReference>
                    </e:ReferenceList>
                </e:EncryptedKey>
                <d:Signature>
                    <d:SignedInfo>
                        <d:CanonicalizationMethod
                            Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                            <x:InclusiveNamespaces
                                PrefixList="d s soapenv ">
                            </x:InclusiveNamespaces>
                        </d:CanonicalizationMethod>
                        <d:SignatureMethod
                            Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1">
                        </d:SignatureMethod>
                        <d:Reference URI="#w_20">
                            <d:Transforms>
                                <d:Transform
                                    Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                    <x:InclusiveNamespaces
                                        PrefixList="s soapenv t u ">
                                    </x:InclusiveNamespaces>
                                </d:Transform>
                            </d:Transforms>
                            <d:DigestMethod
                                Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
                            </d:DigestMethod>
                            <d:DigestValue>
                                8eOcudBlPAL/xCLrwJgrO6u6x6k=
                            </d:DigestValue>
                        </d:Reference>
                        <d:Reference URI="#w_21">
                            <d:Transforms>
                                <d:Transform
                                    Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                    <x:InclusiveNamespaces
                                        PrefixList="soapenv wsu ns2 ">
                                    </x:InclusiveNamespaces>
                                </d:Transform>
                            </d:Transforms>
                            <d:DigestMethod
                                Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
                            </d:DigestMethod>
                            <d:DigestValue>
                                ogiXf7Eqd6w4lUABsc+MKhHX9KQ=
                            </d:DigestValue>
                        </d:Reference>
                        <d:Reference URI="#w_22">
                            <d:Transforms>
                                <d:Transform
                                    Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                    <x:InclusiveNamespaces
                                        PrefixList="s soapenv u ">
                                    </x:InclusiveNamespaces>
                                </d:Transform>
                            </d:Transforms>
                            <d:DigestMethod
                                Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
                            </d:DigestMethod>
                            <d:DigestValue>
                                Ti4TtG7xpmKCUcsCDqKTRV4tNfA=
                            </d:DigestValue>
                        </d:Reference>
                    </d:SignedInfo>
                    <d:SignatureValue>

    Agg/BjAtkLUrwfJK0yPo69pop0Rs00zPf4xP3JXhtEavUFViwj52UnSf38ZVnhVzgGuoiijWdTGV0bx8Bml0saDP0uthBSPtkruD7bxIGgyfNXvErs0uIqVLyHU39bthpL
7eUK2FiSMi42za/iJYJEXaPkK0vrowBDhEiBSC9to=
                    </d:SignatureValue>
                    <d:KeyInfo>
                        <s:SecurityTokenReference>
                            <s:Reference URI="#x509bst_23"
                                ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
x509-token-profile-1.0#X509v3">
                            </s:Reference>
                        </s:SecurityTokenReference>
                    </d:KeyInfo>
                </d:Signature>
            </s:Security>
        </soapenv:Header>
        <soapenv:Body
            xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
            wsu:Id="w_21">
            <e:EncryptedData xmlns:e="http://www.w3.org/2001/04/xmlenc#"
                Id="w_24" Type="http://www.w3.org/2001/04/xmlenc#Content">
                <e:EncryptionMethod
                    Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc">
                </e:EncryptionMethod>
                <e:CipherData>
                    <e:CipherValue>

    Gz+RSMuotReydy+yqxXhgMYcHF2kXt6hrvfeuSWO6C6YIV7M0fE2mtU+crO/C8i7uYadzL3g+Tm7lQOGnyuYNnAXxTcM/QByrAYInJ075j7HWFzYqWiO+lPk2ZzX
weOnV3yPNS3IblnYJxR9/LcSXgghvry0xSsr/pN71URuBQhJaXhxiGAgX3fTdEuZ0NzW33y6Z85naYWszl1DWIOIUMzYaZRSt4ikIz36ktoj9ZMzvZ/9AFakbMeiC2PNAmNTudlc
71PfsCop77p3CaokfPuSiFciO6EOoi/nRs03axnwAdApeQ42QeObBm0nOVK4rw/GL0iuvVtk/dBgIoUrDg==
                    </e:CipherValue>
                </e:CipherData>
            </e:EncryptedData>
        </soapenv:Body>
    </soapenv:Envelope>
```

Figure 10: Thumbprint reference scenario MessagesService request

Scenario 3: Encrypt Thumbprint Reference with Algorithms Suite Basic128Rsa15.

```
<!-- ***********************************************

        Scenario 3: Encrypt Thumbprint reference with Algorithms Suite Basic128Rsa15
        The below MessageService Request is referencing Encrypt KeyInfo using thumbprint reference.
        Request also Signs Timestamp, Body and then Encrypts Body , no Signature encryption.
        Same MessageProtectionOrder for request and responses of sign then encrypt.
        **********************************************************************************************


        POST /MessageService/MessageService HTTP/1.1
        Host: 127.0.0.1:9088
        Accept: application/soap+xml,multipart/related,text/*
        User-Agent: IBM WebServices/1.0
        Cache-Control: no-cache
        Pragma: no-cache
        SOAPAction: "http://www.example.org/getMessage/getMessageOperation"
        Connection: Keep-Alive
        SAVECONNECTION: 8384148411238524943734
        IBM-WAS-CLIENT: TRUE
        Content-Type: text/xml; charset=UTF-8
        Content-Length: 5333
        Date: Tue, 31 Mar 2009 18:42:23 GMT
    -->

    <soapenv:Envelope
        xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
        <soapenv:Header>
            <wsse:Security
                xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
                soapenv:mustUnderstand="1">
                <wsu:Timestamp
                    xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
                    wsu:Id="wssecurity_signature_id_20">
                    <wsu:Created>2009-03-31T18:42:20.625Z</wsu:Created>
                    <wsu:Expires>2009-03-31T18:47:20.640Z</wsu:Expires>
                </wsu:Timestamp>
                <wsse:BinarySecurityToken
                    xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
                    wsu:Id="x509bst_22"
                    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">

    MIICSjCCAbOgAwIBAgIBEjANBgkqhkiG9w0BAQUFADArMQwwCgYDVQQKEwNjYTMxDDAKBgNVBAsTA3NlYzENMAsGA1UEAxMEbXljYTAeFw0wODA5MTYxN
TI0NTVaFw0xMTA2MTMxNTI0NTVaMC4xDTALBgNVBAoTBG15Y28xDTALBgNVBAsTBG15b3UxDjAMBgNVBAMTBWFsaWNlMIGfMA0GCSqGSIb3DQEBAQUAA4GNADC
BiQKBgQDeSazc2OxPpmHgOJJYsIUar6sEEfOzVuYCwhTzPo3OKBUotwWvoH87j27FU863i0rpm6mE1COvPfgsfLxv/5j9MBA57zAisKwGTjKjDCmUGHr6zjpvPIDWzBgRW5qg
y+73rVjM4Q9jdYJ8SYu8Bcsok2D7v2kqAf4keJricK4PnQIDAQABo3sweTAJBgNVHRMEAjAAMCwGCWCGSAGG+EIBDQQfFh1PcGVuU1NMIEdlbmVyYXRlZCBDZXJ0aWZpY2
F0ZTAdBgNVHQ4EFgQU5g/R2lazG391d8Mugsmn7beQcegwHwYDVR0jBBgwFoAUAQB/1l88r1HCu3ZR4OZo3uw/QeowDQYJKoZIhvcNAQEFBQADgYEAmkOAUMpqqCqc
jusQ4GFdRcBev2sH5VHV59+gDbrJz74LozQHlYWhx/Ib32i3Ff6bQ2Lr8+4h0TyT3Sv5qaOA5aTPaklu2e9sS6NM1XvTa7c4Hfb+7c9vqG0JB/J78t8Vg5ZPHsIdEEZxRqA6VrpAH
8FOldacey4w7i5zyBytQgE=
                </wsse:BinarySecurityToken>
                <enc:EncryptedKey
                    xmlns:enc="http://www.w3.org/2001/04/xmlenc#">
                    <enc:EncryptionMethod
                        Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5">
                    </enc:EncryptionMethod>
                    <ds:KeyInfo
                        xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                        <wsse:SecurityTokenReference>
                            <wsse:KeyIdentifier
                                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/oasis-wss-soap-message-
security-1.1#ThumbprintSHA1">
                                JVOTprQ9y6yZKYrezrpTySnnEWo=
                            </wsse:KeyIdentifier>
                        </wsse:SecurityTokenReference>
                    </ds:KeyInfo>
                    <enc:CipherData>
                        <enc:CipherValue>

    AURquVD5YY6nOxm1qmqtPlVm5+0ib6TKViB+ZyYS0Vw5Zjvt8Uox8VGhJxd6KjYHtUEzx47DI/3WklIescEU8fexjNGl0aTzswI1SvrUTL4A+mzDfPAOIq+2ENm3Sp/
aDzOrQ2qSWUgcFn09cFgLTe8L8b4DAkqtAa9qEMMkgyw=
                        </enc:CipherValue>
                    </enc:CipherData>
                    <enc:ReferenceList>
                        <enc:DataReference
                            URI="#wssecurity_encryption_id_23">
                        </enc:DataReference>
                    </enc:ReferenceList>
                </enc:EncryptedKey>
                <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#">
                            <ec:InclusiveNamespaces
                                xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
                                PrefixList="soapenv wsse ds ">
                            </ec:InclusiveNamespaces>
                        </ds:CanonicalizationMethod>
                        <ds:SignatureMethod
                            Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1">
                        </ds:SignatureMethod>
                        <ds:Reference
                            URI="#wssecurity_signature_id_20">
                            <ds:Transforms>
                                <ds:Transform
                                    Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                    <ec:InclusiveNamespaces
                                        xmlns:ec="http://www.w3.org/2001/10/xml-exc-
c14n#"

                                        PrefixList="soapenv wsu wsse ">
                                    </ec:InclusiveNamespaces>
                                </ds:Transform>
                            </ds:Transforms>
                            <ds:DigestMethod
                                Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
                            </ds:DigestMethod>
                            <ds:DigestValue>
                                Q0I63ixk0vR5niQGW/q+/ePXw48=
                            </ds:DigestValue>
                        </ds:Reference>
                        <ds:Reference
                            URI="#wssecurity_signature_id_21">
                            <ds:Transforms>
                                <ds:Transform
                                    Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                    <ec:InclusiveNamespaces
                                        xmlns:ec="http://www.w3.org/2001/10/xml-exc-
c14n#"

                                        PrefixList="soapenv wsu ns2 ">
                                    </ec:InclusiveNamespaces>
                                </ds:Transform>
                            </ds:Transforms>
                            <ds:DigestMethod
                                Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
                            </ds:DigestMethod>
                            <ds:DigestValue>
                                kbA1rCiWejMqSXF7p3vJ7Cy8q6k=
                            </ds:DigestValue>
                        </ds:Reference>
                    </ds:SignedInfo>
                    <ds:SignatureValue>

    G1F8yNdsiW+z+R3ySa4fgDFxydXGEA0Wx4PPlCJMpt+EQqwX/SkheDLU+uGQWUWwjN7K/zuBsKhm1khuiE2z4m1mxdUeFW5ZuxKujxAyEufTeT1+ohKz66VrE
wRfu7yAc0pNb4Vz4kb8po48tDK9YaFnc3cziPhcpt7ajN5DgDE=
                    </ds:SignatureValue>
                    <ds:KeyInfo>
                        <wsse:SecurityTokenReference>
                            <wsse:Reference URI="#x509bst_22"
                                ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
x509-token-profile-1.0#X509v3">
                            </wsse:Reference>
                        </wsse:SecurityTokenReference>
                    </ds:KeyInfo>
                </ds:Signature>
            </wsse:Security>
            <ns2:msgHeaderElement
                xmlns:ns2="http://www.example.org/getMessage/">
                <msgHeaderInput>Header field of Request</msgHeaderInput>
            </ns2:msgHeaderElement>
        </soapenv:Header>
        <soapenv:Body
            xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
            wsu:Id="wssecurity_signature_id_21">
            <enc:EncryptedData
                xmlns:enc="http://www.w3.org/2001/04/xmlenc#"
                Id="wssecurity_encryption_id_23"
                Type="http://www.w3.org/2001/04/xmlenc#Content">
                <enc:EncryptionMethod
                    Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc">
                </enc:EncryptionMethod>
                <enc:CipherData>
                    <enc:CipherValue>

    wtlr61uOK5NQK6xAc9ahyTepikGZOznFi41rFClb6a4k3mB5fm5sOBraPVb0NgYvGhDLZZSP3tYobPkWJKYLNsKmsiO5us4FPIbWeSVR9MCboTj0TZ/uDT/S8S/xlO
PJR0VahXHpS1dh2vV3yGo+NFYcQmBpCKbtVyI82+iKoLOvaARAGvzJ57VpjU6XgIUiETUe5Lcv3Zs0t9MudLSiG2xXtCm/rQ0EuOXLTcazqc23/rfhdSJmLFthEQzujgcQ
                    </enc:CipherValue>
                </enc:CipherData>
            </enc:EncryptedData>
        </soapenv:Body>
    </soapenv:Envelope>
```

Figure 11: Thumbprint reference scenario Message Service response

Scenario 3: Encrypt Thumbprint reference with Basic128Rsa15 Algorithms Suite.
The below is the Response of MessageService call.

```
<!--
        Scenario 3: Encrypt Thumbprint reference with Basic128Rsa15 Algorithms Suite
        The below is the Response of MessageService call with Encrypt KeyInfo using thumbprint reference.
        Response also Signs Timestamp, Body and then Encrypts Body ,  no Signature encryption
        *********************************************************************************************



        HTTP/1.1 200 OK
        Content-Type: text/xml; charset=UTF-8
        Content-Language: en-US
        Content-Length: 4754
        Date: Tue, 31 Mar 2009 18:42:24 GMT
        Server: WebSphere Application Server/7.0
    -->

    <?xml version="1.0" encoding="UTF-8"?>
    <soapenv:Envelope
        xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
        <soapenv:Header>
            <s:Security
                xmlns:s="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
                xmlns:x="http://www.w3.org/2001/10/xml-exc-c14n#"
                xmlns:d="http://www.w3.org/2000/09/xmldsig#"
                xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
                xmlns:e="http://www.w3.org/2001/04/xmlenc#"
                soapenv:mustUnderstand="1">
                <u:Timestamp u:Id="w_20">
                    <u:Created>2009-03-31T18:42:24.671Z</u:Created>
                    <u:Expires>2009-03-31T18:47:24.671Z</u:Expires>
                </u:Timestamp>
                <s:BinarySecurityToken
                    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"
                    u:Id="x509bst_22">

    MIICSDCCAbGgAwIBAgIBEzANBgkqhkiG9w0BAQUFADArMQwwCgYDVQQKEwNjYTMxDDAKBgNVBAsTA3NlYzENMAsGA1UEAxMEbXljYTAeFw0wODA5MTYx
NTI5NTdaFw0xMTA2MTMxNTI5NTdaMCwxDTALBgNVBAoTBG15Y28xDTALBgNVBAsTBG15b3UxDDAKBgNVBAMTA2JvYjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCg
YEAmJSMY3x7aFeiyEaiv22VSKrg5Cj0djPxtoDTqKF2fXawVKF+M2e7PvPyGPeZYqWKG29FiEs0oeL+Mk3Bvu5OEj2ED2srG7KLbae6cDkhV05erkRoIuooaszztv9rEvJ9PQ3W1
SvajHa5njxx7EqhEFQLhjVdQN272jrS+jyTAIcCAwEAAaN7MHkwCQYDVR0TBAIwADAsBglghkgBhvhCAQ0EHxYdT3BlblNTTCBHZW5lcmF0ZWQgQ2VydGlmaWNhdGUwHQ
YDVR0OBBYEFHtz0OUcahe7HIE8F8PwML60N33UMB8GA1UdIwQYMBaAFAEAf9ZfPK9Rwrt2UeDmaN7sP0HqMA0GCSqGSIb3DQEBBQUAA4GBAJUgE9tOGHNpWrCxIZA
+SKLGhF8dmB3Tk08/l8NHPAXC7ZJR4RpaBq7mQM+D5o/Qmn2KneBb0F8fQa4HeG15hg4flk1f2544brkt/8XUVPSG/rAjXG0kIvcAZhj7Ok56JUywbbLt4q3I02IUQkhZ+3wtI
2Xif4c2tHYbSZk5G2Ii
                </s:BinarySecurityToken>
                <e:EncryptedKey>
                    <e:EncryptionMethod
                        Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5">
                    </e:EncryptionMethod>
                    <d:KeyInfo>
                        <s:SecurityTokenReference>
                            <s:KeyIdentifier
                                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/oasis-wss-soap-message-
security-1.1#ThumbprintSHA1">

                                JizrW7Zh0c/TFEdlz1m/VRsW77A=
                            </s:KeyIdentifier>
                        </s:SecurityTokenReference>
                    </d:KeyInfo>
                    <e:CipherData>
                        <e:CipherValue>

    E9kcGtIMK+8LbvGbGMP06/qjD+74/TVcAHf3ToyzUMBPzZJON+IoHRlerVTPam835bKMYziIsuia1TQ9IZJZOm0IRjBUFsnZKL1yQ3tKQ1J7mdGM6g03+OiuPyJ1sy
iAntMGp3Y5iE+YvaxHApgehGvTSYJ5zfAeQrGo63ZGBJc=
                        </e:CipherValue>
                    </e:CipherData>
                    <e:ReferenceList>
                        <e:DataReference URI="#w_23"></e:DataReference>
                    </e:ReferenceList>
                </e:EncryptedKey>
                <d:Signature>
                    <d:SignedInfo>
                        <d:CanonicalizationMethod
                            Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                            <x:InclusiveNamespaces
                                PrefixList="d s soapenv ">
                            </x:InclusiveNamespaces>
                        </d:CanonicalizationMethod>
                        <d:SignatureMethod
                            Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1">
                        </d:SignatureMethod>
                        <d:Reference URI="#w_20">
                            <d:Transforms>
                                <d:Transform
                                    Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                    <x:InclusiveNamespaces
                                        PrefixList="s soapenv u ">
                                    </x:InclusiveNamespaces>
                                </d:Transform>
                            </d:Transforms>
                            <d:DigestMethod
                                Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
                            </d:DigestMethod>
                            <d:DigestValue>
                                IobnhYl6T6/HNY8NE9DtkpZkcBk=
                            </d:DigestValue>
                        </d:Reference>
                        <d:Reference URI="#w_21">
                            <d:Transforms>
                                <d:Transform
                                    Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                    <x:InclusiveNamespaces
                                        PrefixList="soapenv wsu ns2 ">
                                    </x:InclusiveNamespaces>
                                </d:Transform>
                            </d:Transforms>
                            <d:DigestMethod
                                Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
                            </d:DigestMethod>
                            <d:DigestValue>
                                w02QPC5qEkR+GFj1rP/sEbKj4us=
                            </d:DigestValue>
                        </d:Reference>
                    </d:SignedInfo>
                    <d:SignatureValue>

    jEH3ntA4ZMCh6uFZWe1melk1e/Ctg1VyPdTr9jId67ap70qSMFAEn6tnw3ei3iDZdUu0R1l24V/mIF2L6GWw8qL+XDEzXhmgJ/ln7Gs3Q0a0gPVli5prUxsuFeptqp
qjlIv1/6sdH7f8Ew/DdqbGogIU0lbVyeX++gwyQtEzttg=
                    </d:SignatureValue>
                    <d:KeyInfo>
                        <s:SecurityTokenReference>
                            <s:Reference URI="#x509bst_22"
                                ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
x509-token-profile-1.0#X509v3">
                            </s:Reference>
                        </s:SecurityTokenReference>
                    </d:KeyInfo>
                </d:Signature>
            </s:Security>
        </soapenv:Header>
        <soapenv:Body
            xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
            wsu:Id="w_21">
            <e:EncryptedData xmlns:e="http://www.w3.org/2001/04/xmlenc#"
                Id="w_23" Type="http://www.w3.org/2001/04/xmlenc#Content">
                <e:EncryptionMethod
                    Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc">
                </e:EncryptionMethod>
                <e:CipherData>
                    <e:CipherValue>

    iW46gC/XB0QjIv+xHk0FKGCikR4q7TU8fBweNN2s2R0yUS8mjeCgNktkkmHjNceHSAs79iz8Dd0sl7Vz6toMudcLw/NSw5vqSFbsrefN2dhfFtBI2QhbcK+2QbKgjlH
9B3rO4Ta5Ny0OvC7Yvg6gJG3ZhsCNT5dzyDnRzqJM4N8SKFns7rTAnK1y6qx3bN73F2sQzE1R1V7xbGl0dmNuCt7KSPyU1oZBBmB6COKjzbq259Qb9w+/6++cw7eFc9aaUp
R4IheSnDGPfev2lOkb+NJuRDKnAe4aMP1MYLewImKtiRE8nu0WWaQ5REEgOKA3
                    </e:CipherValue>
                </e:CipherData>
            </e:EncryptedData>
        </soapenv:Body>
    </soapenv:Envelope>
```

Figure 12: Signature Confirmation scenario with Encrypted Signature MessagesService request

Scenario 4 (optional): Signature Confirmation with EncryptedSignature, see response. Algorithms Suite Basic128Rsa15.

```
<!--                    **********************************************************
                Scenario 4 (optional): Signature Confirmation.
                                Request includes an Encrypted Signature. The request signs Timestamp,
                                Body. Encrypts Body and entire Signature. Uses Signature encryption.
                                ******************************************************************************************************-->
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd">
  <s:Header>
    <h:msgHeaderElement xmlns:h="http://www.example.org/getMessage/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
      <msgHeaderInput xmlns="">A request header string '1787947221'</msgHeaderInput>
    </h:msgHeaderElement>
    <ActivityId CorrelationId="4834058f-1dd8-451b-bc25-94ae7632d75d" xmlns="http://schemas.microsoft.com/2004/09/ServiceModel/Diagnostics">ba7a9547-
8085-4fe9-995b-459273e5dd0a</ActivityId>
    <o:Security s:mustUnderstand="1" xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
      <u:Timestamp u:Id="uuid-190b9b3a-0bbe-4d25-878b-892873a64ff9-10">
        <u:Created>2009-06-26T00:47:31.521Z</u:Created>
        <u:Expires>2009-06-26T00:52:31.521Z</u:Expires>
      </u:Timestamp>
      <o:BinarySecurityToken>
        <!-- Removed-->
      </o:BinarySecurityToken>
      <e:EncryptedKey Id="_0" xmlns:e="http://www.w3.org/2001/04/xmlenc#">
        <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"></e:EncryptionMethod>
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
          <o:SecurityTokenReference>
            <o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509SubjectKeyIdentifier"
EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-
1.0#Base64Binary">e3PQ5RxqF7scgTwXw/AwvrQ3fdQ=</o:KeyIdentifier>
          </o:SecurityTokenReference>
        </KeyInfo>
        <e:CipherData>
          <e:CipherValue>DUyu.../354=</e:CipherValue>
        </e:CipherData>
        <e:ReferenceList>
          <e:DataReference URI="#_2"></e:DataReference>
          <e:DataReference URI="#_3"></e:DataReference>
        </e:ReferenceList>
      </e:EncryptedKey>
      <e:EncryptedData Id="_3" Type="http://www.w3.org/2001/04/xmlenc#Element" xmlns:e="http://www.w3.org/2001/04/xmlenc#">
        <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"></e:EncryptionMethod>
        <e:CipherData>
          <e:CipherValue>5WMl...SyXc=</e:CipherValue>
        </e:CipherData>
      </e:EncryptedData>
    </o:Security>
    <To s:mustUnderstand="1"
xmlns="http://schemas.microsoft.com/ws/2005/05/addressing/none">http://131.107.153.201/Security_BSP11_Service_WCF/Scenario2.svc/EncryptSignature</To>
    <Action s:mustUnderstand="1"
xmlns="http://schemas.microsoft.com/ws/2005/05/addressing/none">http://www.example.org/getMessage/getMessageOperation</Action>
  </s:Header>
  <s:Body u:Id="_1" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <e:EncryptedData Id="_2" Type="http://www.w3.org/2001/04/xmlenc#Content" xmlns:e="http://www.w3.org/2001/04/xmlenc#">
      <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"></e:EncryptionMethod>
      <e:CipherData>
        <e:CipherValue>RW0t...Qg4A==</e:CipherValue>
      </e:CipherData>
    </e:EncryptedData>
  </s:Body>
</s:Envelope>
```

Figure 13: Signature Confirmation scenario with Encrypted Signature MessagesService response

Scenario 4 (optional): Signature Confirmation with EncryptedSignature.

```
<!--
          ********************************************************
          Scenario 4 (optional): Signature Confirmation.
                    Response includes an Encrypted Signature. The response also Signs Timestamp and
                    Body. Encrypts Body and entire Signature. Uses Signature encryption.
                    *************************************************************************************************** -->
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd">
 <s:Header>
  <ActivityId CorrelationId="9007b11a-5bec-45c1-bbab-6111e242a570" xmlns="http://schemas.microsoft.com/2004/09/ServiceModel/Diagnostics">ba7a9547-
8085-4fe9-995b-459273e5dd0a</ActivityId>
  <o:Security s:mustUnderstand="1" xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
   <u:Timestamp u:Id="uuid-10a4e673-22f3-4575-aa6e-7188da8e52fc-17">
    <u:Created>2009-06-26T00:47:31.551Z</u:Created>
    <u:Expires>2009-06-26T00:52:31.551Z</u:Expires>
   </u:Timestamp>
   <o:BinarySecurityToken>
    <!-- Removed-->
   </o:BinarySecurityToken>
   <e:EncryptedKey Id="_1" xmlns:e="http://www.w3.org/2001/04/xmlenc#">
    <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"></e:EncryptionMethod>
    <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
     <o:SecurityTokenReference>
      <o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509SubjectKeyIdentifier"
EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-
1.0#Base64Binary">5g/R2lazG391d8Mugsmn7beQceg=</o:KeyIdentifier>
     </o:SecurityTokenReference>
    </KeyInfo>
    <e:CipherData>
     <e:CipherValue>sSZ/...H3a4=</e:CipherValue>
    </e:CipherData>
    <e:ReferenceList>
     <e:DataReference URI="#_3"></e:DataReference>
     <e:DataReference URI="#_4"></e:DataReference>
     <e:DataReference URI="#_5"></e:DataReference>
    </e:ReferenceList>
   </e:EncryptedKey>
   <e:EncryptedData Id="_5" Type="http://www.w3.org/2001/04/xmlenc#Element" xmlns:e="http://www.w3.org/2001/04/xmlenc#">
    <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"></e:EncryptionMethod>
    <e:CipherData>
     <e:CipherValue>xfUw...4TYE=</e:CipherValue>
    </e:CipherData>
   </e:EncryptedData>
   <e:EncryptedData Id="_4" Type="http://www.w3.org/2001/04/xmlenc#Element" xmlns:e="http://www.w3.org/2001/04/xmlenc#">
    <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"></e:EncryptionMethod>
    <e:CipherData>
     <e:CipherValue>8khc...aBKg=</e:CipherValue>
    </e:CipherData>
   </e:EncryptedData>
  </o:Security>
 </s:Header>
 <s:Body u:Id="_2" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <e:EncryptedData Id="_3" Type="http://www.w3.org/2001/04/xmlenc#Content" xmlns:e="http://www.w3.org/2001/04/xmlenc#">
   <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"></e:EncryptionMethod>
   <e:CipherData>
    <e:CipherValue>Oq1z...zm8A</e:CipherValue>
   </e:CipherData>
  </e:EncryptedData>
 </s:Body>
</s:Envelope>
```