Technical Specifications for Electronic Business Services (EBS)

Ministry of Health and Long-Term Care

EBS - Generic Security Specification

Version 3.0

Ontario

Table of Contents

Chapter 1 Electronic Business Services (EBS) 3

Glossary 4
Notice to Reader 6
Intended Audience for this Technical Specification Document 7
About This Document 8
Introduction 10
  Certificate Specifications 11
    Master Services Agreement (MSA) 11
    IDP 12
  EBS Web Service Interface 12
  MSA Security Process 13
  IDP Security Process 14
Technical Interface 15
  SOAP Message: 15
  The Message WSDL 15
WS-Security 15
  Identity Requirements 16
  WS-Security Elements Table 16
  Authorization Process 17
  Signing Requirements 17
  Audit Log data elements and format 18
Testing 18
APPENDIX A: Error Codes 19
APPENDIX B: The SOAP Message WSDL Policy Statement 21
APPENDIX C: EBS Header Schema 25
APPENDIX D: MSA Header Schema 26
APPENDIX F: Fault Schema 28
APPENDIX G: SOAP Header MSA Security Model Example 29
APPENDIX H: SOAP Header IDP Security Model Example 33

Chapter 1 Electronic Business Services (EBS)

1

Chapter 1 Electronic Business Services (EBS)

Glossary

Term	Definition
Claim Submission Number (CSN) a.k.a. Billing Number	A unique identifier that is assigned to a Health Care Provider who is registered with MOHLTC for the purpose of submitting claims for insured services.
Digital Certificate	An electronic "identity card" that includes information about: the card holder; the issuer of the certificate; and cryptographic data that enables independent verification of those identities. The certificate includes the public key of the holder, which can be used to verify the source of electronic documents, and to encrypt electronic documents such that they can be decrypted only by the intended recipient.
End User	A Health Information Custodian (HIC) or an agent of a HIC (i.e. employee, 3rd party service provider) acting under the direction and control of the Service User and who is the individual taking the physical steps necessary to invoke an EBS service on behalf of the Service User.
Electronic Medical Record (EMR)	An Electronic Medical Record (EMR) software package - formerly known as Clinical Management System (CMS) - is a system that enables physicians' to store patient administrative/clinical information/charts electronically and is typically interactive. All patient information is stored within the physician's systems/service including the patient Electronic Health Record (EHR). The implication is that this system has interoperability/interconnectivity features built in. An EMR should have the ability to interoperate with other EHRs, hospitals, labs, ministry etc.
GUID	Globally Unique Identifier.
Health Care Provider (HCP)	Individual, group or facility authorized to provide health care services to residents of Ontario.
Health Information Custodian (HIC)	Health Information Custodian as defined in *Personal Health & Information Privacy Act (PHIPA)*.
Ministry Unique Identifier	An identifier assigned by the Ministry of Health and Long-Term Care to individuals or organizations that access ministry services.

Term	Definition
Identity Provider (IDP)	A party or organization that creates, maintains, and manages identity information for *principals* and performs principal authentication for other parties or organizations.
MOHLTC	The Ontario Ministry of Health and Long-Term Care.
Master Services Agreement (MSA)	The binding legal agreement through which MOHLTC accepts the identity of an end user at face value based on authenticating the Service Requestor and Service User at the time of the service request.
PHI	Personal Health Information.
Service Provider (SP)	Throughout this document, Service Provider refers exclusively to MOHLTC, as the provider of a service via EBS.
Service Requestor (SR)	The business entity that sends the Simple Object Access Protocol (SOAP) message to the ministry's web service via EBS on behalf of a user and asserts the identities.
Service User (SU)	The Health Information Custodian (HIC) on whose behalf the web service is being used.
Simple Object Access Protocol (SOAP)	An E**x**tensible **M**arkup **L**anguage (XML)-based protocol for exchanging structured information between computer systems.
Stakeholder Number (SN)	A unique identifier that is assigned to stakeholders of interest who are registered with the MOHLTC.
Trusted Certificate Authority	A third party organization recognized by the Ministry of Health and Long-Term Care as an approved certificate authority.
Web Services Description Language (WSDL)	An XML-based language for describing web services and how to access them. For more information refer to http://www.w3.org/TR/wsdl.
Web Services Security (WS-Security)	An XML based framework for ensuring secure transmission of electronic messages. It will be used for: identification; authentication; and authorization of parties using EBS as well as ensuring message integrity by means of a digital signature applied to each message. For more information refer to http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss.

Notice to Reader

All possible measures are exerted to ensure accuracy of the contents of this manual; however, the manual may contain typographical or printing or other errors. The reader is cautioned against complete reliance upon the contents of the manual without confirming the accuracy and currency of the information contained in it. The Crown in Right of Ontario, as represented by the Ministry of Health and Long-Term Care (MOHLTC), assumes no responsibility for errors or omissions in any of the information contained in this manual, or for any person's use of the material therein, or for any costs or damages associated with such use. In no event shall the Crown in Right of Ontario be liable for any errors or omissions, or for any damages including, without limitation, damages for direct, indirect, incidental, special, consequential or punitive damages arising out of or related to use of information contained in this manual.

This technical specification is intended only to assist and guide the development of software that is compatible with the MOHLTC Electronic Business Services (EBS), a web interface service client application.

Revisions to the specification will be made as required. The ministry will make every effort to give as much advance notice as possible of future revisions. It is essential that software developers keep current regarding any changes to this specification. The current version of the technical specification will be available for download at the following URL:

http://www.health.gov.on.ca/english/providers/pub/pub_menus/pub_ohip.html

- Please direct any questions to the **Service Support Contact Centre (SSCC) at 1 800 262-6524 or** SSContactCentre.MOH@ontario.ca.

Intended Audience for this Technical Specification Document

This document is intended for use by developers of applications and products that support communication with MOHLTC EBS. These services are built to the web services standards detailed in this document.

This document is also intended to be read in the context of either a service agreement between the ministry and the Service Requestor (SR).That is through a Master Service Agreement (MSA) and the appropriate service(s) Schedule(s), (between the ministry and the Service Requestor (SR) or a Service Users (SU)) use of an approved EBS Identity Provider and the acceptance of the appropriate Acceptable Use Policy for the required service(s).

Since the actual message in support of the request for the service via EBS is made by a Service Requestor or a Service User this technical specification is targeted to either of these users.

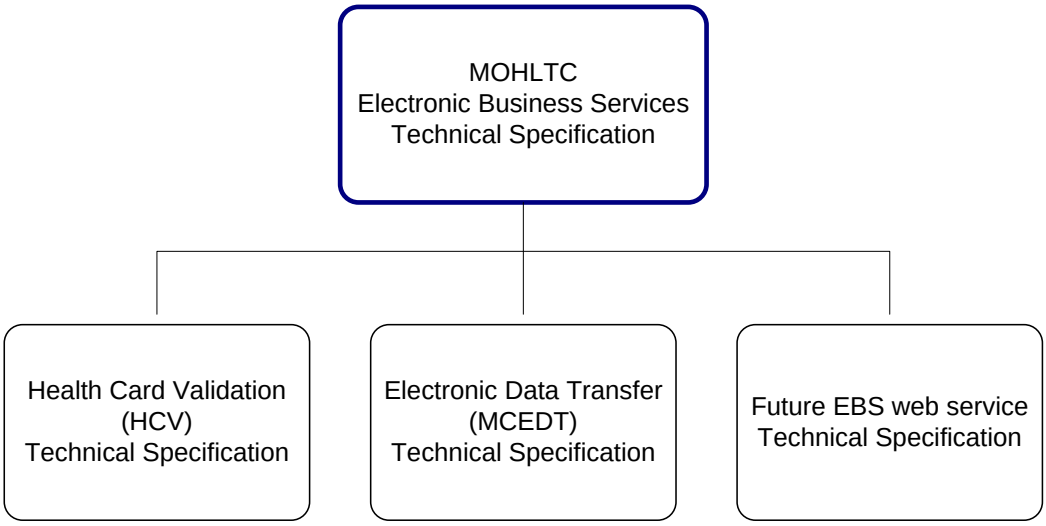
This technical specification is also targeted to vendors of various software applications and products that have or plan to have modules that support EBS through a web service interface within the province of Ontario in Canada.

The document describes the web service, the SOAP message specification and the WS-Security (WSS) specification and aims to guide the users in the development of client applications to integrate with this web service.

It is assumed that the reader has knowledge of web services and related protocols, SOAP and XML message formats/processing, WSS 1.1, relevant interoperability profiles and identity tokens.

About This Document

The Ministry of Health and Long-Term Care provides internet accessible services to health care providers (HCP). This document is intended as the starting point for all web service technical specifications. It outlines the security requirements that all web services may adhere to.



Technical Specification Document Flow Diagram

As such the specifications for individual web services will reside in secondary technical specifications. Designers and developers will need to adhere to the EBS security technical specifications and the appropriate web service specification(s) to be successful in implementing a client for a service.

This document is intended to provide the reader with sufficient information to implement either of the supported EBS security interfaces. All EBS will support one of or both of these security frameworks. For ministry web service specifications a user should consult the appropriate technical specification for that service implementing both the required EBS security interface and the ministry web service interface.

The SOAP Message Section provides the technical specifications of the SOAP message including:

- Message Web Services Description Language (WSDL);

The WS-Security section includes:

- Technical specifications of the WSS 1.1;
- Identity requirements;
- Signing requirements ;
- Encryption requirements; and
- Time stamps.

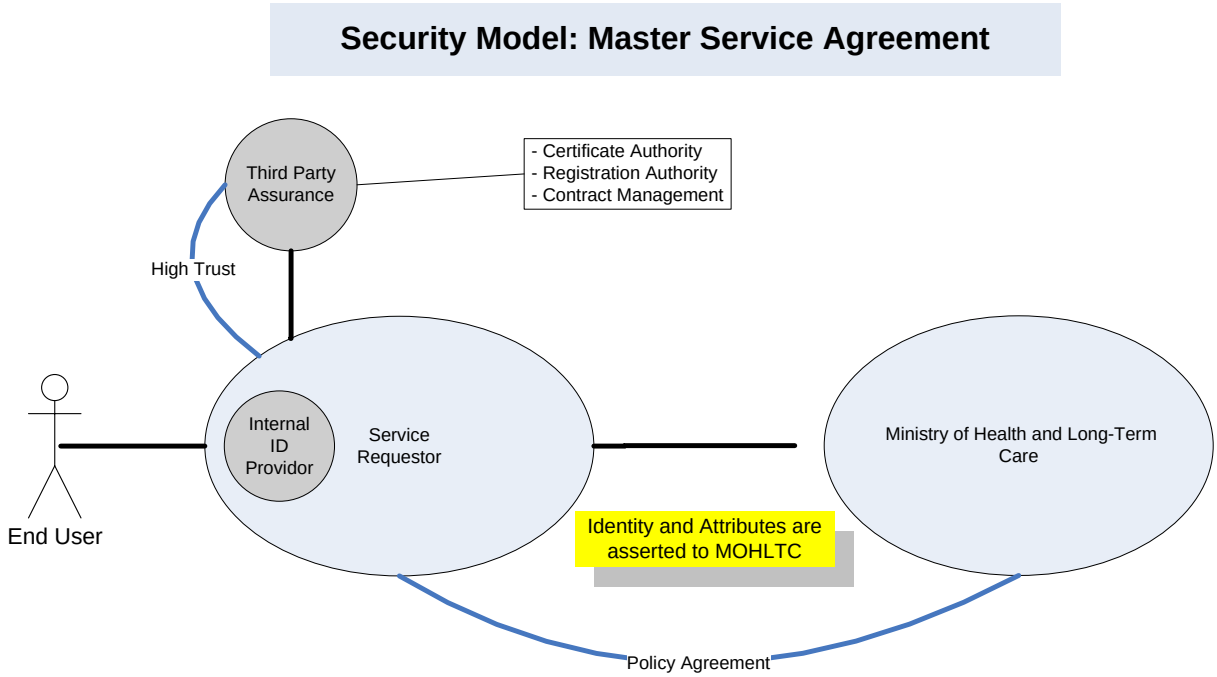
Appendices provide:

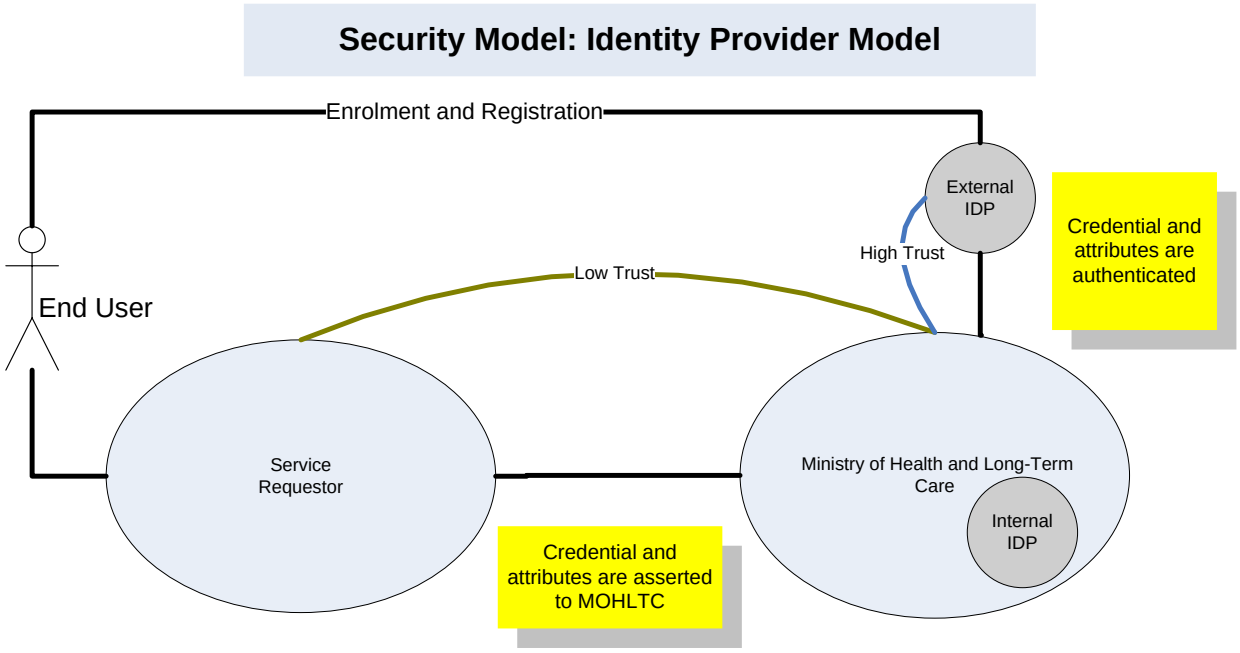
- Error codes;
- EBS Header Element;
- MSA Header Element;
- IDP Header Element;
- EBS Fault Element;
- SOAP Header example.

Introduction

This document represents the first in a series of technical specifications that outline the specification for services under the ministry's EBS initiative. As such this document is the entry point for all technical specifications services' that are provided as part of the EBS. This document outlines the supported security models and the specifications around client software supporting these security models.

There are two supported security models. The first is the Master Services Agreement (MSA) model and the second is the Identity Provider (IDP) model.





All MOHLTC EBS will support one or both security models.

Certificate Specifications

All SOAP messages returned from the EBS systems will be signed using the EBS certificate. Calling systems should verify the signature before accepting any data in the response message.

Master Services Agreement (MSA)

Each Service Requestor (SR) in the MSA model requires a valid certificate from a ministry accepted certificate authority. This certificate must carry a medium level of identity assurance, or on a case by case basis a suitable alternative agreed to by the ministry to be used for any EBS.

To ensure confidentiality and integrity of sensitive information within the message, sender software must use public key technology to sign the SOAP headers and body.

The signing certificate must be issued by a ministry approved authority.

If any response data is specified to be encrypted, by the specific web service technical specification, the data will be encrypted using, at least, the AES128-CBC symmetric encryption algorithm. Symmetric key transport uses the public key belonging to the signer of the initial SOAP request. The encryption algorithm may be increased based on the specific web service technical specification.

IDP

To ensure confidentiality and integrity of sensitive information within the message, sender software must use public key technology to sign the SOAP headers and body.

The signing certificate can be any available certificate and can be self signed.

If any response data is specified to be encrypted, by the specific web service technical specification, the data will be encrypted using, at least, the AES128-CBC symmetric encryption algorithm with the public key belonging to the signer of the initial SOAP request. The encryption algorithm may be increased based on the specific web service technical specification.

EBS Web Service Interface

EBS provides a sustainable, convenient, efficient and secure manner for health service providers and the ministry to send and receive personal health information and establishes a foundation for other electronic service delivery programs.

The EBS considers up to four *roles* in the end to end process of providing services:

Role	Description
Service Provider (SP)	MOHLTC
Service Requestor (SR)	The entity that transmits a service request to MOHLTC. In the MSA agreement model each SR has a Ministry Unique Identifier and this identifier is validated by MOHLTC on each request. In the IDP model the SR is the individual submitting the request and is identified by their IDP credentials.
Service User (SU)	An entity that is a HIC and has its own Ministry Unique Identifier (e.g. Claim Submission Number (CSN) or Stakeholder Number (SN)). This identifier is asserted within the SOAP message and is validated by MOHLTC on each request.
End User	The person who initiates the service request. In the MSA agreement model this end user must be identified within the SR environment. This identifier is generated by the SR and asserted within the SOAP message in support of logging within the service via EBS transaction. In the IDP agreement model this end user is authenticated by the IDP.

MSA Security Process

1. HCP or agent (End User) submits the request into an electronic system (this could be through a hospital Clinical Management System (CMS), an Electronic Medical Record (EMR) or Hospital Information System (HIS), a purpose built application or other).

2. Service User (could be the Service Requestor) submits a request to the Service Requestor on behalf of End User.

3. Service Requestor verifies identity and authorization of Service User and End User.

4. Service Requestor constructs SOAP message using appropriate values and inserts the EBS and MSA headers into the SOAP message header with the Service Requester id in a WS-Security Username token. The SOAP headers and body are then digitally signed to guarantee message integrity and source. If any request data is specified to be encrypted, by the specific web service technical specification, it will use the public key of the EBS system.

5. Service Requestor submits the request.

6. MOHLTC receives the request.

7. MOHLTC verifies message signature, authorizes the asserted identities within message, processes the request and sends the SOAP response back to the Service Requestor.

8. The Service Requestor receives a signed and possibly encrypted data (based on the service) being used message.

9. Service Requestor verifies the message signature, decrypts encrypted data, and makes available the response to Service User and End User as per the agreement between the SR and the Service User.

The web service identifies the entities at each layer based on the identifiers provided through the SOAP headers for the Service Requestor, Service User and End User. These identifiers are expected in specific headers within the SOAP message.

Various scenarios could arise; at one end of the spectrum an entity can assume all the roles (SR, Service User and End User) and at the other end of the spectrum a different entity can assume each of the specified roles.

At the SR level - Ministry Unique Identifier – the SN is expected, and Service User level - a Ministry Unique Identifier – the SN or CSN - is expected. The ministry expects valid identifiers issued by the ministry.

IDP Security Process

1. HCP or agent (End User) submits a request through an electronic system (this could be a hospital Clinical Management System (CMS), an Electronic Medical Record (EMR) or Hospital Information System (HIS), a purpose built application or other).

2. The electronic system constructs a SOAP message using appropriate values and inserts the EBS and IDP headers into the SOAP message header with the user name and password (for the Go-Secure IDP in a WS-Security Username token). The SOAP headers and body are then digitally signed to guarantee message integrity and source. If any request data is specified to be encrypted, by the specific web service technical specification, it will use the public key of the EBS system.

3. MOHLTC receives the request.

4. MOHLTC authenticates the identities within the message, processes the request and sends the response back to the Service Requestor.

5. The Service Requestor receives a signed message.

6. The electronic system verifies the message signature and makes available the response to End User.

The web service identifies the entities at each layer based on the identifiers provided through the SOAP headers for the Service User and End User. These identifiers are expected in specific headers within the SOAP message.

Technical Interface

The Province of Ontario is responsible and accountable for the service provider component.

The service interface uses the SOAP protocol for communication and the WS-Security protocol. There are several implementations of the WS-Security protocol available and it is suggested that one of those be used where possible. The following sections provide detailed descriptions of the SOAP message format and the expected WS-Security elements.

SOAP Message:

SOAP is an XML-based standard protocol that defines a message specification for transmitting XML documents via a network. Since this message specification does not depend on a particular programming language or operating system (OS), data transfer can be conducted among and between systems that use different languages or operating systems.

The Message WSDL

A WSDL is a specification for coding web services-related information (access point and interface specifications, etc.) in XML. Note that while WSDL does not define a protocol when sending/receiving messages, the ministry is using SOAP via HTTPS as the protocol for message transmission.

WS-Security

WS-Security version 1.1 is used for identification, authentication and authorization of the health card validation web service.

The EBS acts as a “Relying Party” and consumes WSS elements provided by accredited Service Requestors.

The SOAP message MUST be signed with a Timestamp element for each message.

Time to live for the SOAP message will be 10 minutes.

Identity Requirements

As part of the WS-Security elements, the caller must include a Username Token.

WS-Security Elements Table

The WSS elements required are:

Element/Attribute	MSA	IDP	Description
Stock Elements			
EBS Header	Y	Y	A mandatory element SOAP header. It contains the software conformance key and the service requestors audit id.
Security Header	Y	Y	A standard WSS Security header with mustUnderstand=”1”.
UsernameToken	Y	Y	For the MSA model this will only consist of the username tag that will contain the Service Requestor id. For the IDP model this will contain both the username and password of the Service User for the Go-Secure IDP.
Timestamp	Y	Y	Specifies the time the message was created and when it expires.
Signature	Y	Y	Digital signature that adheres to the signing requirements specified below.
Custom Attributes			
MSA Header	Y	N	This contains the Service User ministry id and the end user id.
IDP Header	N	Y	This contains the Service User ministry id.

Authorization Process

If a Service Requestor or Service User is not authorized to use the service, a SOAP Fault is returned, including a ministry specific fault code and fault string. (See 'Error Codes' *Appendix A* for more details)

Signing Requirements

The Service Requestor, when producing the SOAP packet, must sign the all headers and the body using a certificate issued by an issuer approved by the Ministry of Health and Long-Term Care.

The digital signature will require:

Attribute	Requirement
Key Identifier Type	Binary Security Token Direct Reference
Signature Canonicalization	http://www.w3.org/2001/10/xml-exc-c14n#
Signature Algorithm	One of: • http://www.w3.org/2000/09/xmldsig#rsa-sha1 • http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 • http://www.w3.org/2001/04/xmldsig-more#rsa-sha384 • http://www.w3.org/2001/04/xmldsig-more#rsa-sha512
Digest Algorithm	One of: • http://www.w3.org/2000/09/xmldsig#sha1 • http://www.w3.org/2001/04/xmldsig-more#sha384 • http://www.w3.org/2001/04/xmlenc#sha256 • http://www.w3.org/2001/04/xmlenc#sha512

Audit Log data elements and format

The Service Requestor is responsible for providing – on demand – audit information describing specific transaction or transaction sequences as identified by the ministry as circumstances dictate. The data that is logged for audit purpose should include at least:

- Transaction id
- Service User
- End User identifier
- Time / date / duration
- Action / event detail
- Simple success or failure
- Exit status / messages
- Error messages

The audit information is to be provided in a comma separated text file.

Testing

All software is required to conformance test with the ministry prior to receiving access to EBS. Any environment changes, including protocol or software changes, or software changes relating to the service interface to the ministry services are also subject to conformance testing.

"Conformance Testing" is the mandatory process of testing performed by all parties that develop software that interface with EBS. This will allow MOHLTC to verify whether the software application complies with each services' Technical Specifications for communication with the ministry's systems before production access is granted. Once this process is completed successfully a software conformance id will be provided by MOHLTC. This id will then need to be sent as part of the WSS elements for each call to EBS.

- Please direct any questions to the **Service Support Contact Centre (SSCC) at 1 800 262-6524 or** SSContactCentre.MOH@ontario.ca.

APPENDIX A: Error Codes

Character based error codes are returned as well as textual descriptions of the error. All ministry specific error codes are 9 characters.

The following are the ministry specific error codes that will be returned in either an EBSFault message or a SOAP Fault message depending on the type of fault. Each fault will be accompanied by brief explanations.

Duplicate comments are intentional.

EBSFault Codes	Error Comment
EHCAU0004	Authorization failed; contact your technical support or software vendor.
EHCAU0011	Service User authorization failed; contact your technical support or software vendor.
EHCAU0012	Service User authorization failed; contact your technical support or software vendor.
EHCAU0013	Authorization failed; contact your technical support or software vendor.
EHCAU0014	Authentication failed; contact your technical support or software vendor.
EHCAU0015	Expired credentials. Password reset may be required; contact your technical support or software vendor.
EHCAU0016	Service Requestor authorization failed; contact your technical support or software vendor.
EHCAU0017	User authorization failed; contact your technical support or software vendor.
EHCAU0018	Service Requestor authorization failed; contact your technical support or software vendor.
EHCAU0019	Service Requestor authorization failed; contact your technical support or software vendor.
EHCAU0020	Service Requestor authorization failed; contact your technical support or software vendor.
EHCAU0021	Authorization failed; contact your technical support or software vendor.

EBSFault Codes	Error Comment
EHCAU0022	Service User authorization failed; contact your technical support or software vendor.
EHCAU0023	Service User authorization failed; contact your technical support or software vendor.
SMIDL0100	System not initialized correctly; contact your technical support or software vendor.
SMIDL0203	Service is not available; contact your technical support or software vendor.
SMIDL0204	General System Error; contact your technical support or software vendor.

SOAP Fault Codes	Error Comment
Rejected By Policy	The SOAP message does not conform to the schema requirements. Detailed description in message.

APPENDIX B: The SOAP Message WSDL Policy Statement

```
<wsp:Policy wsu:Id="request-policy">
	<wsp:ExactlyOne>
		<wsp:All>
			<wsp:All>
				<sp:SignedSupportingTokens>
					<sp:UsernameToken>
						<wsp:Policy>
							<wsp:All>
								<sp:NoPassword/>
								<sp:WssUsernameToken10/>
							</wsp:All>
						</wsp:Policy>
					</sp:UsernameToken>
				</sp:SignedSupportingTokens>
			</wsp:All>
			<wsp:ExactlyOne>
				<wsp:All>
					<sp:RequiredParts>
						<sp:Header Name="EBS" Namespace="http://ebs.health.ontario.ca/"/>
					<sp:RequiredParts>
```

```
                        <sp:RequiredParts>
                              <sp:Header Name="MSA" Namespace="http://msa.ebs.health.ontario.ca/"/>
                        </sp:RequiredParts>
                        <sp:RequiredParts>
                              <sp:Header Name="SoftwareConformanceKey" Namespace=""/>
                        </sp:RequiredParts>
                        <sp:RequiredParts>
                              <sp:Header Name="AuditId" Namespace=""/>
                        </sp:RequiredParts>
                        <sp:RequiredParts>
                              <sp:Header Name="ServiceUserMUID" Namespace=""/>
                        </sp:RequiredParts>
                        <sp:RequiredParts>
                              <sp:Header Name="UserID" Namespace=""/>
                        </sp:RequiredParts>
                        <sp:RequiredParts>
                              <sp:Header Name="Timestamp" Namespace="http://docs.oasis-
                              open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"/>
                        </sp:RequiredParts>
                  </wsp:All>
            </wsp:ExactlyOne>
            <wsp:ExactlyOne>
            <wsp:All>
                  <sp:SignedParts>
                        <sp:Header Name="EBS" Namespace="http://ebs.health.ontario.ca/"/>
                        <sp:Header Name="MSA" Namespace="http://msa.ebs.health.ontario.ca/"/>
                        <sp:Header Name="Timestamp" Namespace="http://docs.oasis-
                        open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"/>
```

```
                        <sp:Header Name="UsernameToken" Namespace="http://docs.oasis-
                        open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"/>
      <sp:Body/>
</sp:SignedParts>
</wsp:All>
</wsp:ExactlyOne>
      <wsp:All>
            <wsp:All>
                  <sp:SignedSupportingTokens>
                        <sp:UsernameToken>
                              <wsp:Policy>
                                    <wsp:All>
                                          <sp:WssUsernameToken10/>
                                    </wsp:All>
                              </wsp:Policy>
                        </sp:UsernameToken>
                  </sp:SignedSupportingTokens>
            </wsp:All>
            <wsp:ExactlyOne>
            <wsp:All>
                  <sp:SignedParts>
                        <sp:Header Name="EBS" Namespace="http://ebs.health.ontario.ca/"/>
                        <sp:Header Name="IDP" Namespace="http://idp.ebs.health.ontario.ca/"/>
                        <sp:Header Name="Timestamp" Namespace="http://docs.oasis-open.org/wss/2004/01/oasis-
                              200401-wss-wssecurity-utility-1.0.xsd"/>
                        <sp:Header Name="UsernameToken" Namespace="http://docs.oasis-
                              open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"/>
                        <sp:Body/>
                  </sp:SignedParts>
            </wsp:All>
```

```
                </wsp:ExactlyOne>
                <wsp:ExactlyOne>
                        <wsp:All>
                                <sp:RequiredParts>
                                        <sp:Header Name="EBS" Namespace="http://ebs.health.ontario.ca/"/>
                                </sp:RequiredParts>
                                <sp:RequiredParts>
                                        <sp:Header Name="IDP" Namespace="http://idp.ebs.health.ontario.ca/"/>
                                </sp:RequiredParts>
                                <sp:RequiredParts>
                                        <sp:Header Name="SoftwareConformanceKey" Namespace=""/>
                                </sp:RequiredParts>
                                <sp:RequiredParts>
                                        <sp:Header Name="AuditId" Namespace=""/>
                                </sp:RequiredParts>
                                <sp:RequiredParts>
                                        <sp:Header Name="ServiceUserMUID" Namespace=""/>
                                </sp:RequiredParts>
                                <sp:RequiredParts>
                                        <sp:Header Name="Timestamp" Namespace="http://docs.oasis-
                                                open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"/>
                                </sp:RequiredParts>
                        </wsp:All>
                </wsp:ExactlyOne>
        </wsp:All>
    </wsp:ExactlyOne>
</wsp:Policy>
```

APPENDIX C: EBS Header Schema

```
<?xml version="1.0" encoding="UTF-8"?><xs:schema targetNamespace="http://ebs.health.ontario.ca/" version="1.0"
       xmlns:tns="http://ebs.health.ontario.ca/"
       xmlns:xs="http://www.w3.org/2001/XMLSchema">

  <xs:element name="EBS" type="tns:ebs_header"/>

  <xs:simpleType name="key">
    <xs:restriction base="xs:string">
          <xs:maxLength value="36"/>
    </xs:restriction>
  </xs:simpleType>

  <xs:simpleType name="uid">
    <xs:restriction base="xs:string">
          <xs:maxLength value="128"/>
    </xs:restriction>
  </xs:simpleType>

  <xs:complexType name="ebs_header">
    <xs:sequence>
      <xs:element minOccurs="1" name="SoftwareConformanceKey" type="tns:key"/>
      <xs:element minOccurs="1" name="AuditId" type="tns:uid"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

APPENDIX D: MSA Header Schema

```
<?xml version="1.0" encoding="UTF-8"?><xs:schema targetNamespace="http://msa.ebs.health.ontario.ca/" version="1.0"
       xmlns:tns="http://msa.ebs.health.ontario.ca/"
       xmlns:xs="http://www.w3.org/2001/XMLSchema">

  <xs:element name="MSA" type="tns:msa_header"/>
  <xs:simpleType name="user">
    <xs:restriction base="xs:string">
        <xs:maxLength value="256" />
    </xs:restriction>
  </xs:simpleType>

  <xs:simpleType name="muid">
    <xs:restriction base="xs:string">
        <xs:maxLength value="10" />
    </xs:restriction>
  </xs:simpleType>

  <xs:complexType name="msa_header">
    <xs:sequence>
      <xs:element minOccurs="1" name="ServiceUserMUID" type="tns:muid"/>
      <xs:element minOccurs="1" name="UserID" type="tns:user"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

APPENDIX E: IDP Header Schema

```
<?xml version="1.0" encoding="UTF-8"?><xs:schema targetNamespace="http://idp.ebs.health.ontario.ca/" version="1.0"
       xmlns:tns="http://idp.ebs.health.ontario.ca/"
       xmlns:xs="http://www.w3.org/2001/XMLSchema">

  <xs:element name="IDP" type="tns:idp_header"/>

  <xs:simpleType name="muid">
    <xs:restriction base="xs:string">
          <xs:maxLength value="10"/>
    </xs:restriction>
  </xs:simpleType>

  <xs:complexType name="idp_header">
    <xs:sequence>
      <xs:element minOccurs="1" name="ServiceUserMUID" type="tns:muid"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

APPENDIX F: Fault Schema

```
<?xml version="1.0" encoding="UTF-8"?><xs:schema targetNamespace="http://ebs.health.ontario.ca/" version="1.0"
       xmlns:tns="http://ebs.health.ontario.ca/"
       xmlns:xs="http://www.w3.org/2001/XMLSchema">

    <xs:element name="EBSFault" type="tns:ebsFault"/>

    <xs:complexType name="ebsFault">
        <xs:sequence>
            <xs:element name="code" type="xs:string"/>
            <xs:element name="message" type="xs:string"/>
        </xs:sequence>
    </xs:complexType>
</xs:schema>
```

APPENDIX G: SOAP Header MSA Security Model Example

```
<soapenv:Header>
    <ns2:EBS wsu:Id="id-1" xmlns:ns2="http://ebs.health.ontario.ca/" >
        <SoftwareConformanceKey>444361ee-277f-7732-c684-7a9923jfgh1b</SoftwareConformanceKey>
        <AuditId>2f8f70fe-400c-49d7-9a02-95ef68bc148e</AuditId>
    </ns2:EBS>
    <ns2:MSA wsu:Id="id-2" xmlns:ns2="http://msa.ebs.health.ontario.ca/" >
        <ServiceUserMUID>4523894</ServiceUserMUID>
        <UserID>walec</UserID>
    </ns2:MSA>
    <wsse:Security SOAP-ENV:mustUnderstand="1">
        <wsu:Timestamp wsu:Id="id-3">
            <wsu:Created>2012-05-31T12:18:14.118Z</wsu:Created>
            <wsu:Expires>2012-05-31T12:18:44.118Z</wsu:Expires>
        </wsu:Timestamp>
        <wsse:UsernameToken wsu:Id="id-4">
            <wsse:Username>73367252</wsse:Username>
        </wsse:UsernameToken>
        <wsse: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"
                wsu:Id="X509-FBB16D2886CB8FE58213384666945491">
                MIICMzCCAZygAwIBAgIET1e+dDANBgkqhkiG9w0BAQUFADBeMQswCQYDVQQGEwJDQTEQMA4GA1UECBMHT250YXJpbzENMAsGA1U
                EChMET0hJUDEVMBMGA1UECxMMUmVnaXN0cmF0aW9uMRcwFQYDVQQDEw4xNDIuMTQ1LjcwLjE3NzAeFw0xMjAzMDcyMDAwNTJaFw
                0xMzAzMDcyMDAwNTJaMF4xCzAJBgNVBAYTAkNBMRAwDgYDVQQIEwdPbnRhcmlvMQ0wCwYDVQQKEwRPSElQMRUwEwYDVQQLEwxSZ
                Wdpc3RyYXRpb24xFzAVBgNVBAMTDjE0Mi4xNDUuNzAuMTc3MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCs/JIP6CE5IkfT
                nD/c56K+QAYqETdLvW1xXJ6ipkVhjjC2ASKuuH4fvhbyxo2B4VugsL9r4E5jHEKoi+GDKOLlLZRfSy0cB8IcpXonAuGqMzhCoEQ
                1CdxNb9etMyvQGRKEBgniKKxTvpTyZdpYDi92up5E+FYL3jEejhp+1iDFJQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAHn8VZS169
                BJMa4E6SNLnY7u80zSh90mbrTUWjM1dEicv3jQMMsrWHfoCt+nRSqfNLUTLc8U0LqiB3jnnNJgJt1T7Sp8eUZPdH0gY3i83ZXA8
                HDFKMZF3qL8I8ncu8FPcZGYBNhYrGjXXsuqXimiTIjxgm06ErRa/51szOFFxWrB
```

```
 </wsse:BinarySecurityToken>
<ds:Signature Id="SIG-6" 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
               PrefixList="SOAP-ENV ebs soap-sec soapenv sp tns wsdl wsp wsse wsu xs xsi"
               xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </ds:CanonicalizationMethod>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
        <ds:Reference URI="#id-1">
            <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                    <ec:InclusiveNamespaces
                     PrefixList="SOAP-ENV ebs soap-sec soapenv sp tns wsdl wsp wsse wsu xs xsi"
                     xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />
                </ds:Transform>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <ds:DigestValue>sKI5sBr8n7rt0GXRxLU2XAIJjBbBKFzQB1Lza0uPw20=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#id-2">
            <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                    <ec:InclusiveNamespaces
                     PrefixList="SOAP-ENV ebs soap-sec soapenv sp tns wsdl wsp wsse wsu xs xsi"
                     xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />
                </ds:Transform>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
```

```
    <ds:DigestValue>RA1O1voUNDV9+hi6IzNNxkTHfEdu2pu6fppiwN23JGI=</ds:DigestValue>
</ds:Reference>
<ds:Reference URI="#id-3">
    <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <ec:InclusiveNamespaces
             PrefixList="SOAP-ENV ebs soap-sec soapenv sp tns wsdl wsp wsse xs xsi"
              xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </ds:Transform>
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
    <ds:DigestValue>pwM8DiAl/JoQarieA1C2Yaj6gao50KBD6vORmlFnJF8=</ds:DigestValue>
</ds:Reference>
<ds:Reference URI="#id-4">
    <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <ec:InclusiveNamespaces
             PrefixList="SOAP-ENV ebs soap-sec soapenv sp tns wsdl wsp wsu xs xsi"
             xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </ds:Transform>
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
    <ds:DigestValue>yFOmFgMDHMBooWIEsB3azib2EX7fR+Ich03J19kFMVE=</ds:DigestValue>
</ds:Reference>
<ds:Reference URI="#id-5">
    <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <ec:InclusiveNamespaces
             PrefixList="SOAP-ENV ebs soap-sec sp tns wsdl wsp wsse wsu xs xsi"
```

```
                        xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />
                    </ds:Transform>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
                <ds:DigestValue>lGKOfXxmbsLds9+tD4eaCObTCdGNXDF/PY9LjDUPl9Y=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>
          X6/PL0ecIyQVX1tFlacQ3Se67uCIp9ZAu677POQNpXCgNO6qMTZZMBZYeC8hS4jcPBCW0dYFvMsDAlbe6i82SgdSEl6QvXB65gIAs
          3QsVaFVdctOnVvMGNfKpMqkXAV5rmtqcOiUNRezNWf9Q3oBBdaM2958tX9qbk3ZG2bCxrU=
        </ds:SignatureValue>
        <ds:KeyInfo Id="KI-FBB16D2886CB8FE58213384666945692">
            <wsse:SecurityTokenReference wsu:Id="STR-FBB16D2886CB8FE58213384666945693">
                <wsse:Reference URI="#X509-FBB16D2886CB8FE58213384666945491"
                  ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
                    1.0#X509v3" />
            </wsse:SecurityTokenReference>
        </ds:KeyInfo>
    </ds:Signature>
</wsse:Security>
</soapenv:Header>
```

APPENDIX H: SOAP Header IDP Security Model Example

```
<soapenv:Header>

<ns2:EBS wsu:Id="id-1" xmlns:ns2="http://ebs.health.ontario.ca/" >
    <SoftwareConformanceKey>444361ee-277f-7732-c684-7a9923jfgh1b</SoftwareConformanceKey>
    <AuditId>35870880-3701-47b7-a34d-439ee754d211</AuditId>
</ns2:EBS>
<ns2:IDP wsu:Id="id-2" xmlns:ns2="http://idp.ebs.health.ontario.ca/" >
    <ServiceUserMUID>4523894</ServiceUserMUID>
</ns2:IDP>
<wsse:Security SOAP-ENV:mustUnderstand="1">
    <wsu:Timestamp wsu:Id="id-3">
        <wsu:Created>2012-06-20T17:58:42.580Z</wsu:Created>
        <wsu:Expires>2012-06-20T17:59:12.580Z</wsu:Expires>
    </wsu:Timestamp>
    <wsse:UsernameToken wsu:Id="id-4">
        <wsse:Username>SUTESTDEVONE@YAHOO.CA</wsse:Username>
        <wsse:Password Type="wsse:PasswordText">Cliffsammy12!</wsse:Password>
    </wsse:UsernameToken>
     <wsse: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"
          wsu:Id="X509-
          02F859690D5C74E20913402151228211">MIICMzCCAZygAwIBAgIET1e+dDANBgkqhkiG9w0BAQUFADBeMQswCQYDVQQGEwJDQTE
          QMA4GA1UECBMHT250YXJpbzENMAsGA1UEChMET0hJUDEVMBMGA1UECxMMUmVnaXN0cmF0aW9uMRcwFQYDVQQDEw4xNDIuMTQ1Ljcw
          LjE3NzAeFw0xMjAzMDcyMDAwNTJaFw0xMzAzMDcyMDAwNTJaMF4xCzAJBgNVBAYTAkNBMRAwDgYDVQQIEwdPbnRhcmlvMQ0wCwYDV
          QQKEwRPSElQMRUwEwYDVQQLEwxSZWdpc3RyYXRpb24xFzAVBgNVBAMTDjE0Mi4xNDUuNzAuMTc3MIGfMA0GCSqGSIb3DQEBAQUAA4
          GNADCBiQKBgQCs/JIP6CE5IkfTnD/c56K+QAYqETdLvW1xXJ6ipkVhjjC2ASKuuH4fvhbyxo2B4VugsL9r4E5jHEKoi+GDKOLlLZR
          fSy0cB8IcpXonAuGqMzhCoEQ1CdxNb9etMyvQGRKEBgniKKxTvpTyZdpYDi92up5E+FYL3jEejhp+1iDFJQIDAQABMA0GCSqGSIb3
          DQEBBQUAA4GBAHn8VZS169BJMa4E6SNLnY7u80zSh90mbrTUWjM1dEicv3jQMMsrWHfoCt+nRSqfNLUTLc8U0LqiB3jnnNJgJt1T7
          Sp8eUZPdH0gY3i83ZXA8HDFKMZF3qL8I8ncu8FPcZGYBNhYrGjXXsuqXimiTIjxgm06ErRa/51szOFFxWrB</wsse:BinarySecur
          ityToken>
```

```
<ds:Signature Id="SIG-6" 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 PrefixList="SOAP-ENV ebs soap-sec soapenv sp tns wsdl wsp wsse wsu xs xsi"
            xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </ds:CanonicalizationMethod>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
        <ds:Reference URI="#id-1">
            <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                    <ec:InclusiveNamespaces
                         PrefixList="SOAP-ENV ebs soap-sec soapenv sp tns wsdl wsp wsse wsu xs xsi"
                         xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />
                </ds:Transform>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <ds:DigestValue>gpejbitTQxuMOhUirdbGNtHjsGhAArhAp3ByFuG9cHs=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#id-2">
            <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                    <ec:InclusiveNamespaces
                         PrefixList="SOAP-ENV ebs soap-sec soapenv sp tns wsdl wsp wsse wsu xs xsi"
                         xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />
                </ds:Transform>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <ds:DigestValue>ZWKvgN+eB0NFmQHPGYN5RoSZzbuboqKLzLcV6PEOz3E=</ds:DigestValue>
        </ds:Reference>
```

```
<ds:Reference URI="#id-3">
    <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <ec:InclusiveNamespaces
                 PrefixList="SOAP-ENV ebs soap-sec soapenv sp tns wsdl wsp wsse xs xsi"
                 xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </ds:Transform>
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
    <ds:DigestValue>1AvUG2EE6+bgpJBe1TB4teUkKD4lRsw69BozDFQMGGE=</ds:DigestValue>
</ds:Reference>
<ds:Reference URI="#id-4">
    <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <ec:InclusiveNamespaces
                 PrefixList="SOAP-ENV ebs soap-sec soapenv sp tns wsdl wsp wsu xs xsi"
                 xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </ds:Transform>
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
    <ds:DigestValue>Lw6C0//TpU0uuta+9pjDPfD0aOokdgbVOEM9eaWcGjo=</ds:DigestValue>
</ds:Reference>
<ds:Reference URI="#id-5">
    <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <ec:InclusiveNamespaces PrefixList="SOAP-ENV ebs soap-sec sp tns wsdl wsp wsse wsu xs xsi"
            xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
            />
        </ds:Transform>
```

```
                    </ds:Transforms>
                    <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
                    <ds:DigestValue>lGKOfXxmbsLds9+tD4eaCObTCdGNXDF/PY9LjDUPl9Y=</ds:DigestValue>
                </ds:Reference>
            </ds:SignedInfo>
                <ds:SignatureValue>
                        Yn5iRnjs/T2+nNgW8pArIgqc445RwL2wYPHZaydVJk0oUXV5B4nzU4fgX/sQTcY0O5vuReP8th4QZoGG6tSnxuBfqiDd2r
                        kRZDrdgotJT++WzhMLdt1J0Kah0aZVCWabQrxeGY2N3QDuMWr5PSlm1RWbkA3W5B4YLaD+S/j3QKc=
                </ds:SignatureValue>
            <ds:KeyInfo Id="KI-02F859690D5C74E20913402151228312">
                <wsse:SecurityTokenReference wsu:Id="STR-02F859690D5C74E20913402151228413">
                        <wsse:Reference URI="#X509-02F859690D5C74E20913402151228211"
                        ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
                        1.0#X509v3" />
                </wsse:SecurityTokenReference>
            </ds:KeyInfo>
        </ds:Signature>
    </wsse:Security>
</soapenv:Header>
```