NATO Communications and Information Agency
Agence OTAN d'information et de communication

AGENCY INSTRUCTION

INSTR TECH 06.02.04

SERVICE INTERFACE PROFILE FOR POLICY ENFORCEMENT POINTS

Effective date:

Revision No: Original

Issued by: Chief, Core Enterprise Services

Approved by: Director Service Strategy

Table of Amendments

Amendment No	Date issued	Remarks

Author Details

Organization	Name	Contact Email/Phone
NCI Agency	R. Fiske	rui.fiske@ncia.nato.int
NCI Agency	M. Lehmann	marek.lehmann@ncia.nato.int
NCI Agency	R. Malewicz	robert.malwicz@ncia.nato.int
NCI Agency	L. Schenkels	leon.schenkels@ncia.nato.int
NCI Agency	D. Gujral	davinder.gujral@ncia.nato.int

Table of Contents

List of Annexes

AGENCY INSTRUCTION 06.02.04

SERVICE INTERFACE PROFILE FOR POLICY ENFORCEMENT POINTS

0 PRELIMINARY INFORMATION

0.1 References

A. NCIA/GM/2012/235; Directive 1 Revision 1; dated 3 May 2013
B. NCIARECCEN-4-22852 DIRECTIVE 01.01, Agency Policy on Management and Control of Directives, Notices, Processes, Procedures and Instructions, dated 20 May 2014
C. NCIARECCEN-4-23297, Directive 06.00.01, Management and Control of Directives, Processes, Procedures and Instructions on Service Management, dated 03 June 2014

0.2 Purpose

This Technical Instruction (TI) provides detailed information, guidance, instructions, standards and criteria to be used when planning, programming, and designing Agency products and services. In this specific case the TI defines a Service Interface Profile (SIP) for one of NATO's Core Enterprise Services.

TIs are living documents and will be periodically reviewed, updated, and made available to Agency staff as part of the Service Strategy responsibility as Design Authority. Technical content of these instructions is the shared responsibility of SStrat/Service Engineering and Architecture Branch and the Service Line of the discipline involved.

TIs are primarily disseminated electronically[1], and will be announced through Agency Routine Orders. Hard copies or local electronic copies should be checked against the current electronic version prior to use to assure that the latest instructions are used.

0.3 Applicability

This TI applies to all elements of the Agency, in particular to all NCI Agency staff involved in development of IT services or software products. It is the responsibility of all NCI Agency Programme, Service, Product and Project Managers to ensure the implementation of this technical instruction and to incorporate its content into relevant contractual documentation for external suppliers.

1 SIP INTRODUCTION

The purpose of this Service Interface Profile (SIP), which should be read along with the Agency Directive 06.05.04.02.H[2], *"Service Interface Profile for Security Services"* [NCIA AD 06.05.04.02.H], is to specify how services may be called that are protected by the Core Enterprise Services (CES) Security Services. This covers only the call from a web service consumer to a web service provider using simple object access protocol (SOAP), and the response from the service provider. This includes how the message must be structured and the elements that must be contained within the call. It does not cover what happens before the call (in other words, how an extensible markup language (XML) *Security Token* is retrieved) or what happens at the *Authorization* stage of the process (contact with the *Policy Decision Point* (*PDP*)). These will be covered by other SIPs.

[1] https://servicestrategy.nr.ncia/SitePages/Agency%20Directives%20(Technical).aspx

[2] The Agency Directive 06.05.04.02.H [NCIA AD 06.05.04.02.H] is also available as the Technical Report with the title *"Security Service Interface Profile (SIP)"* [NCIA TR/2012/CPW007253/02, 2012]

1.1 Notational Conventions

The following notational conventions apply to this document:

- The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [IETF RFC 2119, 1997].
- Words in *italics* indicate terms referenced in Section 1.2.
- `Courier font` indicates syntax derived from the different open standards [OASIS WS-Security, 2006], [W3C WS-Addressing, 2006], [W3C XML-Signature, 2002], [OASIS SAML, 2005], [OASIS SAML Token Profile, 2006], and [WS-I Security, 2010].

1.2 Terminology

The following terminology is used in this SIP and its annexes.

Active Client	A Requestor that is able to make SOAP web service calls directly.
Attributes	Pieces of data concerning entities within a system.
Authentication	The process of establishing the identity of an entity.
Authorization	The process of establishing whether an entity is permitted to perform a particular operation on a resource.
Claims	The Attributes of an entity that are asserted by an entity contained within a Security Token.
Data Consumer	A service or application that calls other services in order to retrieve data.
Data Provider	A service that produces data for other services.
Header	The part of the Message that contains additional information about the message beyond the data that is being exchanged.
Identity Provider (IdP)	An entity that acts as an Authentication service to end-requestors and a data origin Authentication service to service providers. This is typically the role of a Security Token Service.
Message	The structure used for exchanging data between the Data Provider and Data Consumer.
Passive Client	A Requestor that is not able to make SOAP web service calls directly.
Policy Decision Point (PDP)	A service that provides Authorization decisions by evaluating policies against the Attributes of an entity.
Policy Enforcement Point (PEP)	A component that sits in the pipeline of the container of the Data Provider to ensure that security policies are applied.
Relying Party (RP)	This is the service that is protected by the PEP. It relies on the Authentication information presented in the Security Token. It is thus usually the Data Provider.
Requestor	An entity that is making a call to another service.
Security Token	A structure for distributing Claims between entities.
Security Token Service (STS)	A service that issues Security Tokens.

1.3 Relationships to Other Profiles and Specifications

1.3.1 Normative References

In addition to the normative references in the "*Service Interface Profile for Security Services*" [NCIA AD 06.05.04.02.H] the following documents have fed into this specification, and are incorporated as normative references:

1.3.2 Web Services Security: SOAP Message Security 1.1 (OASIS)

http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SOAPMessageSecurity.pdf.

1.3.3 Web Services Security: SAML Token Profile 1.1(OASIS)

http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SAMLTokenProfile.pdf.

1.3.4 Web Services Security: X.509 Certificate Token Profile 1.1(OASIS)

http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-x509TokenProfile.pdf.

2 SIP DEFINITION

2.1 Subject

All services that are protected by the NATO Network Enabled Capability (NNEC) Security Services need to have a common structure for passing identity information to the service container, so that an *Authorization* decision can be reached. This SIP defines that structure, and how messages to services protected in this way must be presented. For a more detailed description of the mechanisms used to protect services, see [NC3A RD-2814, 2009].

2.2 Service Interface

There is no web service description language (WSDL) that is relevant in this situation, as the operations of the service are not constrained by the application of the *PEP*. However, the relevant extract of an auto-generated WSDL, expressed using [OASIS WS-SecurityPolicy, 2009] is contained in Annex 1 .

It is RECOMMENDED that the security policy of a service is not published. However, if the policy is published, then it MUST be published using [OASIS WS-SecurityPolicy, 2009].

2.3 Operations

No operations are specified by this SIP.

2.4 Message Structure

As described in [NCIA TR/2012/CPW007253/02, 2012], the message structure is defined by [NCIA TR/2012/SPW008000/30, 2012]. That is, that the messages MUST be signed, both the requests from *Data Consumer* to *Data Provider*, and the responses from *data provider* to *Data Consumer*. The structures of the messages will be asymmetric, so that the signature from the consumer will be signed using a key from a security assertion markup language (SAML) token (according to the [OASIS SAML Token Profile, 2006]), and the signature from the provider will be signed using the matching asymmetric (private) key for an X.509 binary *Security Token* (according to the [OASIS X.509 Token Profile, 2006]).

2.4.1 Input

2.4.1.1 SOAP Envelope

A request to a service protected by a *PEP* MUST be submitted in a SOAP envelope with a SOAP header element. The version of SOAP to use is not specified by this SIP, but is specified in [NCIA TR/2012/SPW008000/30, 2012].

2.4.1.2 **WS-Addressing Info**

[W3C WS-Addressing, 2006] contains metadata about the message.

2.4.1.2.1 Namespace

Abbreviation	Namespace	Version
wsa	http://www.w3.org/2005/08/addressing	1.0

2.4.1.2.2 Element(s)

Element	Notes
`/soap:Envelope/soap:Header/wsa:Action`	This is REQUIRED, as it is used by the security services as the value of the Action element in the *PDP* request. Its value MUST be signed.
`/soap:Envelope/soap:Header/wsa:MessageID`	This is REQUIRED and MUST be unique for each call to the service. Its value MUST be signed.
`/soap:Envelope/soap:Header/wsa:ReplyTo`	This is OPTIONAL with the default value of: "`http://www.w3.org/2005/08/addressing/anonymous`". This specifies the end-point reference for the intended receiver for replies to this message. A caller MAY explicitly use the anonymous value, "`http://www.w3.org/2005/08/addressing/anonymous`".
`/soap:Envelope/soap:Header/wsa:To`	This is REQUIRED, and is the end-point of the service. Its value MUST be signed.

2.4.1.3 **WS-Security Info**

The [OASIS WS-Security, 2006] element is used to secure the *message*, and contains the signature information for the message, in accordance with the [OASIS SAML Token Profile, 2006]. In addition to those specified in this SIP as mandatory, all important elements of the message SHOULD be signed. The `Security` element also contains the SAML *Security Token* which provides *Claims* about the actor who is trying to call the service. These *Claims* are then included with the authorization request to the *PDP*, prior to evaluating the authorization decision.

2.4.1.3.1 Element(s)

Element	Notes
`/soap:Envelope/soap:Header/ wsse:Security`	This is the element of the SOAP Header that contains all security information, and is therefore REQUIRED.
`/soap:Envelope/soap:Header/ wsse:Security/wsu:Timestamp`	This element specifies the creation date/time and validity of the Message. It is REQUIRED and MUST be signed. The timestamp element MUST be constructed according to Section 7.2 of [WS-I Security, 2010].
`/soap:Envelope/soap:Header/ wsse:Security /ds:Signature`	This contains the signature of elements in the SOAP Message excluding the SAML token, and, as at least some elements of the message will be signed, this is REQUIRED.

2.4.1.4 SAML Assertion

This is a SAML 2.0 assertion, and is used to evaluate the *Authorization* decision for accessing the service. The structure of the SAML assertion is contained in the [NCIA TR/2012/CPW007253/02, 2012].

2.4.1.4.1 Elements (encrypted tokens)

Element	Notes
`/soap:Envelope/soap:Header/wsse: Security/saml:EncryptedAssertion`	If an encrypted token is used.
`/soap:Envelope/soap:Header/wsse: Security/saml:Assertion`	If an unencrypted token is used.

2.4.1.5 Signature

2.4.1.5.1 Element(s)

Element	Notes
`/soap:Envelope/soap:Header/wsse: Security/ds:Signature`	This contains the signature of elements in the SOAP *Message* excluding the SAML token. As at least some elements of the *Message* will be signed, this is REQUIRED. The key used to sign the *Message* MUST be the key specified in the `saml:SubjectConfirmation` element of the SAML assertion.

2.4.1.6 SOAP Body

2.4.1.6.1 Element(s)

Element	Notes
`/soap:Envelope/soap:Body`	This contains the payload of the *Message*. The `Body` MUST be signed.

2.4.2 Outputs

The output will depend on the *Authentication* and *Authorization* decisions of the PEP. If the user is correctly authenticated and authorized, then the PEP will permit the execution of the requested service and will sign the response *message* using the service's X.509 certificate as a binary *Security Token*, according to the [OASIS X.509 Token Profile, 2006].

2.4.2.1 SOAP Envelope

A response from a service protected by a *PEP* MUST be returned in a SOAP envelope with a SOAP *Header* element. The version of SOAP to use is not specified by this directive, but is specified in [NCIA TR/2012/SPW008000/30, 2012].

2.4.2.2 WS-Addressing Info

[W3C WS-Addressing, 2006] contains metadata about the *Message*.

2.4.2.2.1 Element(s)

Element	Notes
`/soap:Envelope/soap:Header/wsa:Action`	This is REQUIRED, as it specifies what action the message is in response to. Its value MUST be signed.
`/soap:Envelope/soap:Header/wsa:RelatesTo`	This is REQUIRED and MUST relate to the corresponding `MessageID` in the request message.

2.4.2.3 WS-Security Info

The [OASIS WS-Security, 2006] element is used to secure the message, and contains the signature information for the message, and the binary *Security Token* of the service (the service's X.509 certificate). In addition to those specified in this SIP as mandatory, all important elements of the message SHOULD be signed. It is REQUIRED that the *Security Token* is included directly in the `<wsse:Security>` element to avoid the recipient having to retrieve the certificate from elsewhere. The token MUST be an X.509 v3 token.

2.4.2.3.1 Element(s)

Element	Notes
`/soap:Envelope/soap:Header/wsse:Security`	This is the element of the SOAP *Header* that contains all security information, and is therefore REQUIRED. It is from WS-Security 1.0, though is part of WS-Security 1.1.
`/soap:Envelope/soap:Header/wsse:Security/wsu:Timestamp`	This element specifies the creation date/time and validity of the *Message*. It is REQUIRED and MUST be signed.
`/soap:Envelope/soap:Header/wsse:Security/wsse:BinarySecurityToken`	This is the Base64-encoded representation of the certificate that is used to sign the response *Message*, which identifies the service provider. It is therefore REQUIRED.
`/soap:Envelope/soap:Header/wsse:Security/wsse:BinarySecurityToken/@valueType`	This specifies the type of token to use, and so MUST have a value of: `http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3`.
`/soap:Envelope/soap:Header/wsse:Security/ds:Signature`	This contains the signature of elements in the SOAP *Message*, and, as at least some elements of the *Message* will be signed, this is REQUIRED. The key used to sign the *Message* MUST be the private key matching the certificate in the `wsse:BinarySecurityToken` element.

2.4.2.4 SOAP body

2.4.2.4.1 Element(s)

Element	Notes
`/soap:Envelope/soap:Body`	This contains the actual data of the *Message*. The `Body` MUST be signed.

2.4.3 Errors

There are many security-related errors that may be raised as SOAP faults by the *PEP*. The actual errors will depend on the implementation of the *PEP*. However, the RECOMMENDED list, drawn from [OASIS WS-Security, 2006], [OASIS SAML Token Profile, 2006] is as follows:

Assertion processing error	RECOMMENDED error (fault code)
An unsupported token was provided	`wsse:UnsupportedSecurityToken`
An unsupported signature or encryption algorithm was used	`wsse:UnsupportedAlgorithm`
An error was discovered processing the `<wsse:Security>` header.	`wsse:InvalidSecurity`
An invalid security token was provided	`wsse:InvalidSecurityToken`
The security token could not be authenticated or authorized	`wsse:FailedAuthentication`
The signature or decryption was invalid	`wsse:FailedCheck`
Referenced security token could not be retrieved	`wsse:SecurityTokenUnavailable`
The message has expired	`wsse:MessageExpired`
A referenced SAML assertion could not be retrieved.	`wsse:SecurityTokenUnavailable`
An assertion contains a <saml:Condition> element that the receiver does not understand.	`wsse:UnsupportedSecurityToken`
A signature within an assertion or referencing an assertion is invalid.	`wsse:FailedCheck`
The issuer of an assertion is not acceptable to the receiver.	`wsse:InvalidSecurityToken`
The receiver does not understand the extension schema used in an assertion.	`wsse:UnsupportedSecurityToken`
The receiver does not support the SAML version of a referenced or included assertion.	`wsse:UnsupportedSecurityToken`

3 REFERENCES

[NC3A RD-2814, 2009]:
NATO Consultation, Command and Control Agency Reference Document 2814, "Bi-SC AIS/NNEC SOA Implementation Guidance" *(provisional title)*, J. Busch, S. Brown, R. Fiske, G. Hallingstad, M. Lehman, NC3A, The Hague, Netherlands, unpublished document dated December 2009 (NATO Unclassified).

[NCIA AD 06.05.04.02.H]
NATO Communications and Information Agency, Agency Directive 06.05.04.02.H, "Service Interface Profile for Security Services", R. Fiske, M. Lehmann, R. Malewicz, L. Schenkels, D. Gujral, NCIA, The Hague, Netherlands, to be published, (NATO Unclassified)

[NCIA TR/2012/CPW007253/02, 2012]:
NATO Communications and Information Agency Technical Report 2012/CPW007253/02, "Security Services Service Interface Profile Proposal", R. Fiske, M. Lehmann, R. Malewicz, L. Schenkels, D. Gujral, NCIA, The Hague, Netherlands, October 2012 (NATO Unclassified).

[NCIA TR/2012/SPW008000/30, 2012]:
NATO Communications and Information Agency Technical Report 2012/SPW008000/30, "Messaging Service Interface Profile Proposal", R. Fiske, M. Lehmann, NCIA, The Hague, Netherlands, October 2012 (NATO Unclassified).

[OASIS SAML Token Profile, 2006]:
Organization for the Advancement of Structured Information Standards (on-line), http://www.oasis-open.org, Web Services Security: SAML Token Profile 1.1, at http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SAMLTokenProfile.pdf, 1 February 2006, viewed 30 March 2011.

[OASIS X.509 Token Profile, 2006]:
Organization for the Advancement of Structured Information Standards (on-line), http://www.oasis-open.org, Web Services Security: X.509 Certificate Token Profile 1.1, at http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-x509TokenProfile.pdf, 1 February 2006, viewed 30 March 2011.

[OASIS WS-Security, 2006]:
Organization for the Advancement of Structured Information Standards (on-line), http://www.oasis-open.org, Web Services Security: SOAP Message Security 1.1, at http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SOAPMessageSecurity.pdf, 1 February 2006, viewed 30 March 2011.

[OASIS WS-SecurityPolicy, 2009]:
Organization for the Advancement of Structured Information Standards (on-line), http://www.oasis-open.org, WS-SecurityPolicy 1.3, at http://docs.oasis-open.org/ws-sx/ws-securitypolicy/v1.3/ws-securitypolicy.html, 2 February 2009, viewed 30 March 2011.

[W3C WS-Addressing, 2006]:
World Wide Consortium (on-line), http://www.w3.org, Web Services Addressing 1.0 – Core, at http://www.w3.org/TR/2006/REC-ws-addr-core-20060509/, 9 May 2006, viewed 30 March 2011.

[WS-I Security, 2010]:
Web Services Interoperability Organization (on-line), http://www.ws-i.org, Basic Security Profile Version 1.1, at http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html, 24 January 2010, viewed 30 March 2011.

4 ABBREVIATIONS

CES	Core Enterprise Services
PDP	Policy decision point
PEP	Policy enforcement point
SAML	Security assertion markup language
SIP	Service interface profile
SOAP	Simple object access protocol
XML	Extensible markup language

ANNEX 1 – XML SAMPLES

1.1 NON-NORMATIVE WSDL, including WS-Security Policy Fragment for Service

```
<wsdl:definitions  name="..Service  Name.."  targetNamespace="http://tempuri.org/"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"      xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:wsam="http://www.w3.org/2007/05/addressing/metadata"
xmlns:tns="http://tempuri.org/"
xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
xmlns:wsap="http://schemas.xmlsoap.org/ws/2004/08/addressing/policy"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:msc="http://schemas.microsoft.com/ws/2005/12/wsdl/contract"
xmlns:wsaw="http://www.w3.org/2006/05/addressing/wsdl"
xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
xmlns:wsa10="http://www.w3.org/2005/08/addressing"
xmlns:wsx="http://schemas.xmlsoap.org/ws/2004/09/mex">
  <wsp:Policy wsu:Id="..Service Policy ID..">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:AsymmetricBinding
xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:InitiatorToken>
              <wsp:Policy>
                <sp:IssuedToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/A
lwaysToRecipient">
                  <Issuer
xmlns="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
                    <Address    xmlns="http://www.w3.org/2005/08/addressing">..Issuer
Endpoint..</Address>
                    <Metadata xmlns="http://www.w3.org/2005/08/addressing">
                      <Metadata     xmlns="http://schemas.xmlsoap.org/ws/2004/09/mex"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
                        <wsx:MetadataSection xmlns="">
                          <wsx:MetadataReference>
                            <Address
xmlns="http://www.w3.org/2005/08/addressing">..Issuer Mex Endpoint..</Address>
                          </wsx:MetadataReference>
                        </wsx:MetadataSection>
                      </Metadata>
                    </Metadata>
                    <Identity
xmlns="http://schemas.xmlsoap.org/ws/2006/02/addressingidentity">
                      <Dns>">..Issuer Servername..</Dns>
                    </Identity>
                  </Issuer>
                  <sp:RequestSecurityTokenTemplate>
                    <t:TokenType
xmlns:t="http://schemas.xmlsoap.org/ws/2005/02/trust">http://docs.oasis-
open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0</t:TokenType>
                    <t:KeyType
xmlns:t="http://schemas.xmlsoap.org/ws/2005/02/trust">http://schemas.xmlsoap.org/ws/
2005/02/trust/PublicKey</t:KeyType>
                  </sp:RequestSecurityTokenTemplate>
                  <wsp:Policy>
                    <sp:RequireInternalReference/>
                  </wsp:Policy>
                </sp:IssuedToken>
```

```
            </wsp:Policy>
          </sp:InitiatorToken>
          <sp:RecipientToken>
            <wsp:Policy>
              <sp:X509Token
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/A
lwaysToInitiator">
                <wsp:Policy>
                  <sp:WssX509V3Token10/>
                </wsp:Policy>
              </sp:X509Token>
            </wsp:Policy>
          </sp:RecipientToken>
          <sp:AlgorithmSuite>
            <wsp:Policy>
              <sp:Basic256/>
            </wsp:Policy>
          </sp:AlgorithmSuite>
          <sp:Layout>
            <wsp:Policy>
              <sp:Lax/>
            </wsp:Policy>
          </sp:Layout>
          <sp:IncludeTimestamp/>
          <sp:OnlySignEntireHeadersAndBody/>
        </wsp:Policy>
      </sp:AsymmetricBinding>
      <sp:Wss11 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
        <wsp:Policy>
          <sp:MustSupportRefKeyIdentifier/>
          <sp:MustSupportRefIssuerSerial/>
          <sp:MustSupportRefThumbprint/>
          <sp:MustSupportRefEncryptedKey/>
        </wsp:Policy>
      </sp:Wss11>
      <sp:Trust10 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
        <wsp:Policy>
          <sp:MustSupportIssuedTokens/>
          <sp:RequireClientEntropy/>
          <sp:RequireServerEntropy/>
        </wsp:Policy>
      </sp:Trust10>
      <wsaw:UsingAddressing/>
    </wsp:All>
  </wsp:ExactlyOne>
</wsp:Policy>
<wsp:Policy wsu:Id="..Service Input Policy..">
  <wsp:ExactlyOne>
    <wsp:All>
      <sp:SignedParts
xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
        <sp:Body/>
        <sp:Header Name="To" Namespace="http://www.w3.org/2005/08/addressing"/>
        <sp:Header Name="From" Namespace="http://www.w3.org/2005/08/addressing"/>
        <sp:Header                                                    Name="FaultTo"
Namespace="http://www.w3.org/2005/08/addressing"/>
        <sp:Header                                                    Name="ReplyTo"
Namespace="http://www.w3.org/2005/08/addressing"/>
        <sp:Header                                                  Name="MessageID"
Namespace="http://www.w3.org/2005/08/addressing"/>
        <sp:Header                                                  Name="RelatesTo"
Namespace="http://www.w3.org/2005/08/addressing"/>
        <sp:Header                                                    Name="Action"
Namespace="http://www.w3.org/2005/08/addressing"/>
```

```
        </sp:SignedParts>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy wsu:Id="..Service Output Policy..">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SignedParts
xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <sp:Body/>
          <sp:Header Name="To" Namespace="http://www.w3.org/2005/08/addressing"/>
          <sp:Header Name="From" Namespace="http://www.w3.org/2005/08/addressing"/>
          <sp:Header                                                    Name="FaultTo"
Namespace="http://www.w3.org/2005/08/addressing"/>
          <sp:Header                                                    Name="ReplyTo"
Namespace="http://www.w3.org/2005/08/addressing"/>
          <sp:Header                                                  Name="MessageID"
Namespace="http://www.w3.org/2005/08/addressing"/>
          <sp:Header                                                  Name="RelatesTo"
Namespace="http://www.w3.org/2005/08/addressing"/>
          <sp:Header                                                    Name="Action"
Namespace="http://www.w3.org/2005/08/addressing"/>
        </sp:SignedParts>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsdl:import namespace="..Service Namespace.." location="..WSDL URL.."/>
  <wsdl:types/>
  <wsdl:binding name="..Binding Name.." type="..Service Type..">
    <wsp:PolicyReference URI="#..Service Policy (ref).."/>
    <soap:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="..Service Operation..">
      <soap:operation soapAction="..SOAP Action URI.." style="document"/>
      <wsdl:input>
        <wsp:PolicyReference URI="#..Service Input Policy (ref).."/>
        <soap:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <wsp:PolicyReference URI="#..Service Output Policy (ref).."/>
        <soap:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:service name="..Service Name..">
    <wsdl:port name="..Port Name.." binding="..Port QName..">
      <soap:address location="..Service Endpoint.."/>
      <wsa10:EndpointReference>
        <wsa10:Address>..Service Endpoint..</wsa10:Address>
        <Identity xmlns="http://schemas.xmlsoap.org/ws/2006/02/addressingidentity">
          <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
            <X509Data>
              <X509Certificate>..Service                Base64                Encoded
Certificate..</X509Certificate>
            </X509Data>
          </KeyInfo>
        </Identity>
      </wsa10:EndpointReference>
    </wsdl:port>
  </wsdl:service>
</wsdl:definitions>
```

1.2 NON-NORMATIVE Message Samples

1.2.1 Request Messages

1.2.1.1 Encrypted SAML Token

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:wsa="http://www.w3.org/2005/08/addressing" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
  <soap:Header>
    <wsa:Action soap:mustUnderstand="1" wsu:Id="_2">..SOAP Action..</wsa:Action>
    <wsa:MessageID wsu:Id="_3">urn:uuid:3f0a9442-417b-4ea4-9b1e-
eefcb25266ad</wsa:MessageID>
    <wsa:ReplyTo wsu:Id="_4">
      <wsa:Address>http://www.w3.org/2005/08/addressing/anonymous</wsa:Address>
    </wsa:ReplyTo>
    <wsa:To soap:mustUnderstand="1" wsu:Id="_5">..Service Endpoint..</wsa:To>
    <wsse:Security soap:mustUnderstand="1" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
      <wsu:Timestamp wsu:Id="uuid-0c947d60-1347-4295-bb4b-3d6a543fa2c0-32">
        <wsu:Created>2010-11-23T09:38:26.460Z</wsu:Created>
        <wsu:Expires>2010-11-23T09:43:26.460Z</wsu:Expires>
      </wsu:Timestamp>
      <EncryptedAssertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
        <xenc:EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
          <xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"></xenc:EncryptionMethod>
          <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
            <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
              <xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
                <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
              </xenc:EncryptionMethod>
              <KeyInfo>
                <ds:X509Data xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                  <ds:X509IssuerSerial>
                    <ds:X509IssuerName>..Cert Issuer..</ds:X509IssuerName>
                    <ds:X509SerialNumber>..Cert Ref..</ds:X509SerialNumber>
                  </ds:X509IssuerSerial>
                </ds:X509Data>
              </KeyInfo>
              <xenc:CipherData>
                <xenc:CipherValue>..Encrypted Key..</xenc:CipherValue>
              </xenc:CipherData>
            </xenc:EncryptedKey>
          </KeyInfo>
          <xenc:CipherData>
            <xenc:CipherValue>..Encrypted SAML Token..</xenc:CipherValue>
          </xenc:CipherData>
        </xenc:EncryptedData>
      </EncryptedAssertion>
      <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#hmac-
sha1"></SignatureMethod>
          <Reference URI="#_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>yyrUshkAm5rOS8y727VkDT+czPg=</DigestValue>
          </Reference>
          <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>mDOSw3rJFnYX2u2/EpWnzo1LqxQ=</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>AGdrIE+6OY1PjPkT6exyNOi/7+I=</DigestValue>
          </Reference>
          <Reference URI="#_4">
            <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>l6mMmQ2LE9VFtjaA6Qc4GKBXURw=</DigestValue>
          </Reference>
          <Reference URI="#_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>bScCfoF9LLXw1zbbsg5jxeTFBxI=</DigestValue>
          </Reference>
          <Reference URI="#uuid-0c947d60-1347-4295-bb4b-3d6a543fa2c0-32">
            <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>SIDZHVf/tAHA9QASWCTCb2NjMDs=</DigestValue>
          </Reference>
        </SignedInfo>
        <SignatureValue>vZgvnJqssls9dPLRJDOFjW/1Bu0=</SignatureValue>
        <KeyInfo>
          <wsse:SecurityTokenReference b:TokenType="http://docs.oasis-
open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0" xmlns:b="http://docs.oasis-
open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd">
            <wsse:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-
wss-saml-token-profile-1.1#SAMLID">_629652e0-6ef2-46e3-852d-
5d859fb44731</wsse:KeyIdentifier>
          </wsse:SecurityTokenReference>
        </KeyInfo>
      </Signature>
    </wsse:Security>
  </soap:Header>
  <soap:Body wsu:Id="_1">
    ..SOAP Body..
  </soap:Body>
</soap:Envelope>
```

1.2.1.2 Unencrypted SAML Token

```
<soap:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:wsa="http://www.w3.org/2005/08/addressing" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
  <soap:Header>
    <wsa:Action soap:mustUnderstand="1" wsu:Id="_2">..SOAP Action..</</wsa:Action>
    <wsa:MessageID wsu:Id="_3">urn:uuid:14a78884-e5a4-451e-8707-
b63e3f88bee3</wsa:MessageID>
    <wsa:ReplyTo wsu:Id="_4">
      <wsa:Address>http://www.w3.org/2005/08/addressing/anonymous</wsa:Address>
    </wsa:ReplyTo>
    <wsa:To soap:mustUnderstand="1" wsu:Id="_5">..Service Endpoint..</wsa:To>
    <wsse:Security soap:mustUnderstand="1" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
      <wsu:Timestamp wsu:Id="uuid-2ee1805f-7251-4203-b877-c5266e238424-6">
        <wsu:Created>2010-11-23T12:14:18.783Z</wsu:Created>
        <wsu:Expires>2010-11-23T12:19:18.783Z</wsu:Expires>
      </wsu:Timestamp>
      <Assertion ID="_e3534d1e-a301-462c-ad72-46fe56c995c8" IssueInstant="2010-11-
23T12:14:18.382Z" Version="2.0" xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
        <Issuer>..Token Issuer..</Issuer>
        <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#"></ds:CanonicalizationMethod>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-
more#rsa-sha256"></ds:SignatureMethod>
            <ds:Reference URI="#_e3534d1e-a301-462c-ad72-46fe56c995c8">
              <ds:Transforms>
                <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"></ds:Transform>
                <ds:Transform Algorithm="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:DigestMethod>

<ds:DigestValue>C4uizWDjuFgPlRf9Eh8G6ssZsVByFp7rSf9Gd+butds=</ds:DigestValue>
            </ds:Reference>
          </ds:SignedInfo>
          <ds:SignatureValue>>..Signature Value..</ds:SignatureValue>
          <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
            <ds:X509Data>
              <ds:X509Certificate>..Base64 Encoded Issuer
Certificate..</</ds:X509Certificate>
            </ds:X509Data>
          </KeyInfo>
        </ds:Signature>
        <Subject>
          <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-
key">
            <SubjectConfirmationData wsa:type="KeyInfoConfirmationDataType"
xmlns:wsa="http://www.w3.org/2001/XMLSchema-instance">
              <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
                  <xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
                    <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
                  </xenc:EncryptionMethod>
                  <KeyInfo>
```

```
                    <ds:X509Data xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                      <ds:X509IssuerSerial>
                        <ds:X509IssuerName>..Cert Issuer..</ds:X509IssuerName>
                        <ds:X509SerialNumber>..Cert Ref..</ds:X509SerialNumber>
                      </ds:X509IssuerSerial>
                    </ds:X509Data>
                  </KeyInfo>
                  <xenc:CipherData>
                    <xenc:CipherValue>..Encrypted Key..</xenc:CipherValue>
                  </xenc:CipherData>
                </xenc:EncryptedKey>
              </KeyInfo>
            </SubjectConfirmationData>
          </SubjectConfirmation>
        </Subject>
        <Conditions NotBefore="2010-11-23T12:14:18.368Z" NotOnOrAfter="2010-11-
23T13:14:18.368Z">
          <AudienceRestriction>
            <Audience>..Relying Party URI..</Audience>
          </AudienceRestriction>
        </Conditions>
        <AttributeStatement>
          <Attribute Name="http://schemas.xmlsoap.org/claims/UPN">
            <AttributeValue>
              ..Value from Directory..
            </AttributeValue>
          </Attribute>
          <Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">
            <AttributeValue>
              ..Value from Directory..
            </AttributeValue>
            <AttributeValue>
              ..Value from Directory..
            </AttributeValue>
          </Attribute>
          <Attribute Name="http://schemas.xmlsoap.org/claims/EmailAddress">
            <AttributeValue>
              ..Value from Directory..
            </AttributeValue>
          </Attribute>
        </AttributeStatement>
        <AuthnStatement AuthnInstant="2010-11-23T12:14:18.315Z">
          <AuthnContext>

<AuthnContextClassRef>urn:federation:authentication:windows</AuthnContextClassRef>
          </AuthnContext>
        </AuthnStatement>
      </Assertion>
      <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#hmac-
sha1"></SignatureMethod>
          <Reference URI="#_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>oc4JWy9Wqw3df1jfkiRMGiKSYLE=</DigestValue>
          </Reference>
```

```
          <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>mDOSw3rJFnYX2u2/EpWnzo1LqxQ=</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>cq4lcqtr41Z1ia4pBb0IjbHn1Qw=</DigestValue>
          </Reference>
          <Reference URI="#_4">
            <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>l6mMmQ2LE9VFtjaA6Qc4GKBXURw=</DigestValue>
          </Reference>
          <Reference URI="#_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>bScCfoF9LLXw1zbbsg5jxeTFBxI=</DigestValue>
          </Reference>
          <Reference URI="#uuid-2ee1805f-7251-4203-b877-c5266e238424-6">
            <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>oOcZSNsbQvpG7wTfiKmSMxMSL34=</DigestValue>
          </Reference>
        </SignedInfo>
        <SignatureValue>FRDWNv6S/vJ+RNgE4b2B86U+r80=</SignatureValue>
        <KeyInfo>
          <wsse:SecurityTokenReference b:TokenType="http://docs.oasis-
open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0" xmlns:b="http://docs.oasis-
open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd">
            <wsse:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-
wss-saml-token-profile-1.1#SAMLID">_e3534d1e-a301-462c-ad72-
46fe56c995c8</wsse:KeyIdentifier>
          </wsse:SecurityTokenReference>
        </KeyInfo>
      </Signature>
    </wsse:Security>
  </soap:Header>
  <soap:Body wsu:Id="_1">
    ..SOAP Body..
  </soap:Body>
</soap:Envelope>
```

1.2.2 Response Message

```
<soap:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:wsa="http://www.w3.org/2005/08/addressing" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
  <soap:Header>
    <wsa:Action soap:mustUnderstand="1" wsu:Id="_1">..SOAP Action..</wsa:Action>
    <wsa:RelatesTo wsu:Id="_2">urn:uuid:3f0a9442-417b-4ea4-9b1e-
eefcb25266ad</wsa:RelatesTo>
    <wsse:Security soap:mustUnderstand="1" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
      <wsu:Timestamp wsu:Id="uuid-cd438e11-9203-47f6-aeca-82627f043364-2">
        <wsu:Created>2010-11-23T09:38:32.678Z</wsu:Created>
        <wsu:Expires>2010-11-23T09:43:32.678Z</wsu:Expires>
      </wsu:Timestamp>
      <wsse:BinarySecurityToken>
        ..Base64 Encoded Service Certificate..
      </wsse:BinarySecurityToken>
      <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="#_0">
            <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>x5N5bNmu3K1BPDi40ZoFVM0Epk0=</DigestValue>
          </Reference>
          <Reference URI="#_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>7UQ6FVRZdVH1/nZp6CxUNY4lae8=</DigestValue>
          </Reference>
          <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>BGxl1wQG5v3dujGMJgO5Zr/sV8U=</DigestValue>
          </Reference>
          <Reference URI="#uuid-cd438e11-9203-47f6-aeca-82627f043364-2">
            <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>AZNpHeZNcdSTMIA9Yhn39Kap8gE=</DigestValue>
          </Reference>
        </SignedInfo>
        <SignatureValue>>..Signature Value..</SignatureValue>
        <KeyInfo>
          <wsse:SecurityTokenReference>
```

```
            <wsse:Reference URI="#uuid-3c9ed799-e278-4b0d-9048-abfed9b963d7-
13"></wsse:Reference>
          </wsse:SecurityTokenReference>
        </KeyInfo>
      </Signature>
    </wsse:Security>
  </soap:Header>
  <soap:Body wsu:Id="_0">
    ..SOAP Body..
  </soap:Body>
</soap:Envelope>
```