OSCI-Transport, Version 2.0

– Web Services Profiling and Extensions Specification –

OSCI Steering Office

Status: Final
Edition 1, published 4st of June, 2009

This is the approved final version of the OSCI 2.0 Web Services Profiling and Extensions Specification. Minor clarifications may be eligible, which could result from perceptions made in the implementation and/or rollout process. These will be published in future editions of this document.

The latest edition always will be available at www.osci.eu/transport/OSCI2/specification.

Editor of this document:

Jörg Apitzsch, bos bremen online services GmbH & Co. Kg, ja@bos-bremen.de

Quality Assurance:

Thilo Schuster, cit GmbH, thilo.schuster@cit.de

Further contributors are listed in [Appendix D.].

Comments and questions may be addressed to the above mentioned persons.

Change History (since Edition 1)

Edition	as of	Author	Changes made / Comments

Table of Contents

1 Introduction

The Web Services Profiling and Extensions Specification **O**nline **S**ervice **C**omputer **I**nterface Transport 2.0 (OSCI 2.0) is made up of five documents:

(1) "OSCI-Transport 2.0 – Functional Requirements and Design Objectives“

(2) "OSCI-Transport 2 – Technical Features Overview"

(3) "OSCI Transport 2.0 – General Architecture“

and

(4) "OSCI Transport 2.0 – Web Services Profiling and Extensions Specification“.

These for documents are accomplished by a common comprehensive glossary:

(5) "OSCI Transport 2 – Glossary“.

While the technical overwie and the specification and profiling documents are presented in English language only, the other mentioned documents initially are available in German language[1].

The background and principles of the **O**nline **S**ervice **C**omputer **I**nterface (OSCI) Tranport spefiction is explained in the document "OSCI-Transport 2 – Technical Features Overview", which should be read first to obtain a base understanding for the profiling and specifications outlined in the here presented document.

[1] While the here presented document is under composition, the English translations of the document „OSCI Transport 2.0 – Generelle Architektur” (general Architecture) is still outstanding.

2 Document Structure

Chapter [3] clarifies formal appointments concerning notational conventions, which is followed by a summary of conformance targets and requirements.

Due to the proliferation of differing platforms and technologies in the eGovernment, it is essential to ensure the different Web Service implementations are interoperable, regardless of the underlying implementation and operation technology. Therefore, we mainly rely on the work which is done by the Web Services Interoperability Organization[2], where profilings are compiled of the major Web Services specifications under the aspect of best practices for Web Services interoperability. If needed to satisfy the underlying OSCI requirements, we define further restrictions and processing rules in addition to these profilings. This is outlined in the chapters [5 thru 7].

As OSCI Transport has to serve special requirements, which are not yet satisfied by currently available Web Services specifications, chapter [8] specifies extensions to the WS-Stack for these purposes.

Chapter [9] summarizes the constituent of the different OSCI message types, completed by hints concerning policies and metadata definitions for nodes and endpoints of OSCI-based communication networks in chapter [10].

Finally, in chapter [11] hints are given to realize services, which may be needed by applications for end-to-end encryption and digital signature services on the content data level. Although a transport protocol should be agnostic to payload carried, these services are needed to satisfy confidentiality, legal bindings and non repudiation requirements.

In a continuing refinement process, this specification will be amended by example policies and realization hints for selected classes of communication scenarios.

[2] see http://www.ws-i.org/

3 Document Conventions

3.1 Notational Conventions

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 [RFC2119].

This specification uses the following syntax to define normative outlines for messages:

- The syntax appears as an XML instance, but values in italics indicate data types instead of values.
- Characters are appended to elements and attributes to indicate cardinality:
  - "?" (0 or 1)
  - "*" (0 or more)
  - "+" (1 or more)
- The character "|" is used to indicate a choice between alternatives.
- The characters "(" and ")" are used to indicate that contained items are to be treated as a group with respect to cardinality or choice.
- An ellipsis (i.e. "...“) indicates a point of extensibility that allows other child or attributes content specified in this document. Additional children elements and/or attributes MAY be added at the indicated extension points but they MUST NOT contradict the semantics of the parent and/or owner, respectively. If an extension is not recognized it SHOULD be ignored.
- XML namespace prefixes (see section 3.2) are used to indicate the namespace of the element being defined.

Elements and Attributes defined by this specification are referred to in the text of this document using [XPATH 1.0] expressions. Extensibility points are referred to using an extended version of this syntax:

- An element extensibility point is referred to using {any} in place of the element name. This indicates that any element name can be used, from any namespace other than the osci: namespace.
- An attribute extensibility point is referred to using @{any} in place of the attribute name. This indicates that any attribute name from any namespace can be used.

For those parts of this specification where referenced specifications are profiled, normative statements of requirements are presented in the following manner:

Rnnnn - *Statement text here*

where "nnnn" is replaced by a number that is unique among the requirements in this specification, thereby forming a unique requirement identifier.

The terms “header" and “body" used in this document are used as abbreviation of “SOAP header" respective “SOAP body".

Following legend applies for the message diagrams in this docuement:

- Mandatory constituents have continuous lines, optional ones are marked dashed.
- Arrows on the left diagram side mark transport encryption requirements, those on the right transport signature requirements.
- Encrypted message parts are marked by a hatched background.

182 For explanation of used abbreviations and terms see the additional document "OSCI Transport 2.0 –
183 Glossary“.

184 3.2 XML Namespaces

185 Following XML namespaces are referenced:

Prefix	XML Namespace	Specification
ds	**http://www.w3.org/2000/09/xmldsig#**	[XMLDSIG]
dss	**urn:oasis:names:tc:dss:1.0:core:schema**	[DSS]
fimac	**urn:de:egov:names:fim:1.0:authenticationcontext**[3]	[SAFE]
osci	**http://www.osci.eu/ws/2008/05/transport**	This document
s12	**http://www.w3.org/2003/05/soap-envelope**	[SOAP12]
samlac	**urn:oasis:names:tc:SAML:2.0:ac**	[SAMLAC]
saml2	**urn:oasis:names:tc:SAML:2.0:assertion**	[SAML2]
wsa	**http://www.w3.org/2005/08/addressing**	[WSA]
wsaw	**http://www.w3.org/2006/05/addressing/wsdl**	[WSAW]
wsdli	**http://www.w3.org/ns/wsdl-instance**	[WSDL20]
wsdl11	**http://schemas.xmlsoap.org/wsdl/**	[WSDL11]
wsmc	**http://docs.oasis-open.org/ws-rx/wsmc/200702**	[WSMC]
wsp	**http://www.w3.org/ns/ws-policy**	[WSPF], [WSPA]
wspmtom	**http://docs.oasis-open.org/ws-rx/wsrm/200702**	[MTOMP]
wsrm	**http://docs.oasis-open.org/ws-rx/wsrm/200702**	[WSRM]
wsrmp	**http://docs.oasis-open.org/ws-rx/wsrmp/200702**	[WSRMP]
wsse	**http://docs.oasis-open.org/wss/oasis-wss-wsecurity-secext-1.1.xsd**	[WSS]
wssp	**http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702**	[WSSP]
wsu	**http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd**	[WSS10]
wst	**http://docs.oasis-open.org/ws-sx/ws-trust/200512**	[WST]
xenc	**http://www.w3.org/2001/04/xmlenc#**	[XENC]

[3] Preliminary namespace for a SAML AuthnContext extension; proposual subject to standardization in Germany

xkms	**http://www.w3.org/2002/03/xkms#**	[XKMS]
xkmsEU	**http://www.lsp.eu/2009/04/xkmsExt#**	[XKMSEU]
xs	**http://www.w3.org/2001/XMLSchema**	[XMLSchema]

186 Table 1: Referenced Namespaces

4 Specification Conformance

4.1 Conformance Requirements

An implementation is not conformant with this specification if it fails to satisfy one or more of the MUST, MUST NOT or REQUIRED level requirements defined herein.

A SOAP node MUST NOT use following XML namespace identifiers for the custom SOAP headers defined in this specification within SOAP envelopes unless it is conformant with this specification:

- **`http://www.osci.eu/ws/2008/05/osci-transport.xsd`**
- **`http://www.w3.org/2002/03/xkms#`**
- **`http://www.osci.eu/2008/05/common/xkiss_ext_de.xsd`.**

Normative text within this specification takes precedence over normative outlines, which in turn take precedence over the [XMLSchema] descriptions.

4.2 Conformance Targets

Conformance targets identify what artefacts (e.g., SOAP message, WSDL description, security token) or parties (e.g., SOAP processor, end user) requirements apply to.

This allows for the definition of conformance in different contexts, to assure unambiguous interpretation of the applicability of requirements, and to allow conformance testing of artefacts (e.g., SOAP messages and WSDL descriptions) and the behaviour of various parties to a Web Service (e.g., clients and service instances).

Requirements' conformance targets are physical artefacts wherever possible, to simplify testing and avoid ambiguity.

The following conformance targets are used in this specification:

OSCI MESSAGE - protocol elements that profiles the SOAP Envelope, whereby following special OSCI message types are defined:

osci:Request, osci:Response, MsgBoxFetchRequest, MsgBoxResponse, MsgBoxStatusListRequest, MsgBoxGetNextRequest, MsgBoxCloseRequest

OSCI GATEWAY – an assembly of functionalities realized in software able to produce, send, receive and consume OSCI Messages, hereby not concerned with SOAP Body entries (OSCI Messages for MsgBox access and faults transmitted in the SOAP body excepted)

DESCRIPTION - descriptions of types, messages, interfaces and their concrete protocol and data format bindings, and the network access points associated with Web Services (e.g., WSDL descriptions)

INITIATOR – end point instance that generates a message according to the protocol associated with it and that sends it to a RECIPIENT or MsgBox potentially through a message path that involves one or multiple INTERMEDIARY(ies);

RECIPIENT – end point instance that consumes a message according to the protocol associated with it.

INTERMEDIARY – node instance in the message path to the RECIPIENT which offers surplus to the MESSAGE according to the protocol associated with it.

MSG-BOX SERVICE (short **MsgBox**) **–** specialized INTERMEDIARY instance that is able to relay messages until they are pulled by the intended RECIPIENT according to the protocol defined here.

227 **ENDPOINT** – collective term for INITIATOR, RECIPIENT and MsgBox. Each ENDPOINT may be in
228 the role of a Security Token Requestor (STR)

229 **STR –** Security Token Requestor as defined by WS-Trust.

230 **STS –** Security Token Service as defined by WS-Trust.

231 **SAML-TOKEN –** Security Token as defined by SAML.

5 SOAP Version, Transport and Fault Binding

R0010 - **OSCI Nodes** MUST support SOAP Version 1.2 according to [SOAP12] and constraints specified in [WSI-Basic], chapter 3 Messaging with restriction R0020.

R0020 - Transport binding is restricted to HTTP/1.1, which has performance advantages and is more clearly specified than HTTP/1.0. R1140 of [WSI-Basic] (A MESSAGE SHOULD be sent using HTTP/1.1) – is superseded: A **MESSAGE** MUST be sent using HTTP/1.1.

Note that this requirement does not prohibit the use of HTTPS.

R0030 - Errors use the SOAP fault mechanisms. The SOAP fault block according to [SOAP12] MUST be used to report information about errors occurring while processing a SOAP/OSCI message. The **`s12:Fault`** element MUST be carried in the SOAP body block of the network backchannel SOAP response message or – if no backchannel available in asynchronous scenarios – in the SOAP body block of a distinct message of osci:Request.

As specifications incorporated here in general define their own fault handling, this document only outlines additional fault situations specific to OSCI Transport.

Following information for the sub elements **`s12:Fault`** is supplied per fault described in this document:

Sub Element	Property Label	Possible values
`/Fault/Code/Value`	[Code]	Sender | Receiver
`/Fault/Code/Value/Subcode`	[Subcode]	A local QName assigned to the fault
`/Fault/Reason/Text`	[Reason]	The English language reason explanation

In the fault message itself, the [Code] value MUST have a prefix of **`s12:`**; the [Subcode] value prefix MUST be **`osci:`**.

It should be noted that implementations MAY provide second-level details fields, but they should be careful not to introduce security vulnerabilities when doing so (e.g. by providing too detailed information).

6 Addressing Endpoints

The use of WS-Addressing with SOAP 1.2-binding and WS-Addressing Metadata is mandatory for OSCI Transport.

R0100 - **OSCI Nodes** MUST support WS-Addressing and WS-Addressing Metadata according to [WSA] and [WSAM]. Constraints apply specified in [WSI-Basic], chapter 3.6 "Support for WS-Addressing Messaging" and chapter 3.7 "Use of WS-Addressing MAPs".

R0110 - **OSCI Nodes** MUST support WS-Addressing SOAP Binding according to [WSASOAP], whereby only the rules for binding to SOAP 1.2 apply.

6.1 Use of WS-Addressing

The use of mechanisms specified by WS-Addressing [WSA] is REQUIRED. The use of WS-Addressing MUST be expressed in the syntax defined by WS-Addressing metadata [WSAM] in the WSDL describing and endpoint (see chapter [10]).

6.1.1 Endpoint Reference

WS-Addressing introduces the construct of endpoint references (EPR) and defines abstract properties for one-way and request-response MEPs (see [WSA] , chapter 3.1), whereas OSCI regularly uses request-response MEPs. The XML Infoset representation is given in [WSA] , chapter 3.2.
This specification defines following restrictions on the cardinality of elements contained in a type of **`wsa:EndpointReference`** and concretion concerning the element **`wsa:ReferenceParameters:`**

```
<wsa:EndpointReference>
   <wsa:Address> xs:anyURI </wsa:Address>
   <wsa:ReferenceParameters>
   <osci:TypeOfBusinessScenario> xs:anyURI</osci:TypeOfBusinessScenario>
   </wsa:ReferenceParameters> ?
   <wsa:Metadata>
     (  xmlns:wsdli="http://www.w3.org/ns/wsdl-instance"
         wsdli:wsdlLocation= "xs:anyURI xs:anyURI"> ) |
       xs:any *
    </wsa:Metadata> ?
</wsa:EndpointReference>
```

`/wsa:ReferenceParameters`

R0120 – If the URI value of …/wsa:Address is not equal to **"`http://www.w3.org/2005/08/addressing/anonymous`"**, an EPR MUST contain one element **`wsa:ReferenceParameters`** which carries the type of business scenario addressed by the message. This element is defined as type xs:any* and optional in [WSA]. The type of business scenario MUST be tagged as URI in the OSCI namespace as osci:TypeOfBusinessScenario.

Any endpoint SHOULD expose the types of business scenarios which it actually is able to serve in WSDL [WSDL11] format. An XML schema definition for the Content Data to be carried in the SOAP body of the message MUST be bound to the concrete tagged type of business scenario. Following the WSDL binding of WS-Addressing [WSAW], each **`osci:TypeOfBusinessScenario`** corresponds to a specific port [WSDL11] respective endpoint [WSDL20].

300 Following types of business scenarios MUST be served by all OSCI endpoints:

Type of business scenario URI	Meaning
http://www.osci.eu/2008/common/urn/messageTypes/Receipt	Receipt type messages
http://www.osci.eu/2008/common/urn/messageTypes/Notification	Notification type messages
http://www.osci.eu/2008/common/urn/messageTypes/Fault	Fault type messages

301 Table 2: Predefined business scenario types

302 Following type of business scenerio SHOULD be served by OSCI endpoints, which are
303 intended to be able to support a common mail-style data exchange, optional carrying any
304 type of attachments[4]:

305 **http://www.osci.eu/2008/common/urn/messageTypes/LetterStyle**

306 **/wsa:MetaData**

307 R0130 - an EPR MAY have elements **/wsa:MetaData** which carry embedded or
308 referenced metadata information assigned to this EPR.

309 Each OSCI endpoint SHOULD publish a link to its WSDL by using
310 **wsdli:wsdlLocation**.

311 Such elements form the metadata that is relevant to the interaction with the endpoint. An
312 Initiator MUST have knowledge about following metadata specific for OSCI about the
313 destination he is targeting a message to, at least each OSCI endpoint SHOULD publish
314 references to its encryption and signature certificate(s) in the OSCI specifc policy
315 **/osci:X509CertificateAssertion**[5] by using the
316 **wsse:SecurityTokenReference/wsse:Reference** token reference.

317 X.509-Certificate to be used for end-to-end encryption of Content Data as exposed in
318 **/osci:X509CertificateAssertion.**

319 X.509-Certificate to possibly to be used for transport encryption (depending on concrete
320 security policy) as exposed in **/osci:X509CertificateAssertion.**

321 X.509-Certificates used by the destination for receipt signatures, possibly those used for
322 cryptographic time stamping, too (both exposed in
323 **/osci:X509CertificateAssertion).**

324 Availability of qualified time stamping service and policies those apply here (as exposed in
325 /**osci:QualTSPAssertion**[6]**.**

326 Possible rules applied by the destination concerning message lifetime, if messages are
327 marked as valid for a restricted period of time (see chapter [8.1] for this issue; the
328 endpoint behaviour id outlined in the /**osci:ObsoleteAfterAssertion**[6] of the OSCI
329 spefic policy.

[4] The according content data schema will be made available as addendum short after publishing of this specification

[5] Details are defined in chapter [10.2.1]

[6] See chapter [10.2.2]

These requirements and capabilities of an OSCI endpoint have SHOULD be described as policies in machine readable form; for details, see chapter [10.2]. It is advised to carry URI-references to these policies in **/wsa:MetaData**. Anyway, it is possible to embed these policies in any WSDL (fragment) describing the OSCI endpoint or even to exchange these information on informal basis out of scope of this specification.

6.1.2 Addressing Properties – SOAP Binding

This specification defines following restrictions on the cardinality of WS-Addressing message addressing properties carried as SOAP header elements as outlined in Web Services Addressing 1.0 – SOAP Binding [WSASOAP]:

```
<wsa:To> xs:anyURI </wsa:To>
<wsa:ReferenceParameters>xs:any*</wsa:ReferenceParameters>
<wsa:From> wsa:EndpointReferenceType </wsa:From> ?
<wsa:ReplyTo> wsa:EndpointReferenceType </wsa:ReplyTo> ?
<wsa:FaultTo> wsa:EndpointReferenceType </wsa:FaultTo> ?
<wsa:Action>
   http://www.osci.eu/ws/2008/05/transport/urn/messageTypes/OSCIRequest |
   http://www.osci.eu/ws/2008/05/transport/urn/messageTypes/OSCIResponse |
   http://www.osci.eu/ws/2008/05/transport/urn/messageTypes/MsgBoxFetchRequ
est |
   http://www.osci.eu/ws/2008/05/transport/urn/messageTypes/MsgBoxStatusLis
tRequest|
   http://www.osci.eu/ws/2008/05/transport/urn/messageTypes/MsgBoxResponse
     |
   http://www.osci.eu/ws/2008/05/transport/urn/messageTypes/MsgBoxGetNextRe
quest |
   www.osci.eu/ws/2008/05/transport/urn/messageTypes/MsgBoxCloseRequest
</wsa:Action>
<wsa:MessageID> xs:anyURI </wsa:MessageID>
<wsa:RelatesTo RelationshipType="xs:anyURI"?>xs:anyURI</wsa:RelatesTo> *
```

/wsa:To

The message final destination URI defined in **wsa:Address** is mapped to this SOAP header element which MUST be provided exactly once.

/wsa:ReferenceParameters (mapped to **osci:TypeOfBusinessScenario** in the SOAP binding)

R0140 - an OSCI message MUST carry at least one element according to the SOAP mapping defined for **wsa:ReferenceParameters**. According to R0120, this is an URI carried in a SOAP header element **osci:TypeOfBusinessScenario** which is bound to the address element **wsa:To**. The SOAP header **osci:TypeOfBusinessScenario** MUST carry an attribute **wsa:IsReferenceParameter="true".**

If this header element is missing or the addressed endpoint is not able to serve the concrete **osci:TypeOfBusinessScenario,** a fault MUST be generated and the message MUST be discarded:

Fault 1: AddrWrongTypeOfBusinessScenario
[Code] Sender
[Subcode] AddrWrongTypeOfBusinessScenario
[Reason] Type of Business Scenario missing or not accepted

/wsa:From ?

As OSCI is designed for authoritative communication, an OSCI message SHOULD carry at most one SOAP header element **wsa:From** of type **wsa:EndpointReferenceType**. If carried, the issuer of this message MUST expose here the EPR where he is able to

accept osci:Request messages according to R0120, R0130; it SHOULD carry the same entries as **/wsa:ReplyTo.**

In case of an anonymous Initiator this EPR MAY contain the only child element **wsa:Address** with a content of **"http://www.w3.org/2005/08/addressing/anonymous".**

/wsa:ReplyTo ?

R0150 - in case of non-anonymous and/or asynchronous scenarios a messages of type osci:Request MUST carry exactly one SOAP header element **wsa:ReplyTo** of type **wsa:EndpointReferenceType.** This MUST contain the concrete EPR of the endpoint according to R0120, R0130; it denotes the final destination the Recipient MUST deliver the response to. The **wsa:ReferenceParameters** of this EPR SHOULD be the same as bound to the address element **wsa:To.**

If this element is not supplied, the osci:Response (or a fault) is delivered in the http-backchannel (semantics following [WSA], anonymous URI).

For sake of simplification, all other OSCI message types SHOULD NOT carry this SOAP header element, as for these message types reply destinations are defaulted to the anonymous URI or there is no need to generate related responses at all.

/wsa:FaultTo ?

R0160 - If faults related to this message shall not (or cannot in asynchronous scenarios) be delivered in the network connection backchannel or it is intended to route such fault messages to specialized endpoints for consuming fault messages, an OSCI message SHOULD carry this optional element **wsa:FaultTo** of type **wsa:EndpointReferenceType.** This MUST be a concrete EPR according to R1020, R0130. To distinct such messages from other message types, the **wsa:ReferenceParameters** of this EPR MUST be

<osci:TypeOfBusinessScenario>
www.osci.eu/2008/common/urn/messageTypes/Fault
</osci:TypeOfBusinessScenario>

In this case, a http response code of 500 MUST be returned in the backchannel of the SOAP request and the body of the SOAP response MUST carry the fault information in parallel to the fault message send to the endpoint denoted in **/wsa:FaultTo.**

If this element is not supplied, the fault only MUST be delivered in the http-backchannel.

/wsa:Action

R0170 - this mandatory element of type **xs:anyURI** denotes the type of the OSCI message and MUST carry one of the values outlined in the table below. An OSCI message MUST carry exactly one **/wsa:Action** SOAP header element.

wsa:Action URIs assigned to OSCI Message Types
http://www.osci.eu/ws/2008/05/transport/urn/messageTypes/osci:Request
http://www.osci.eu/ws/2008/05/transport/urn/messageTypes/osci:Response
http://www.osci.eu/ws/2008/05/transport/urn/messageTypes/MsgBoxFetchRequest
http://www.osci.eu/ws/2008/05/transport/urn/messageTypes/MsgBoxStatusListRequest

http://www.osci.eu/ws/2008/05/transport/urn/messageTypes/MsgBoxResponse
http://www.osci.eu/ws/2008/05/transport/urn/messageTypes/MsgBoxGetNextRequest
http://www.osci.eu/ws/2008/05/transport/urn/messageTypes/MsgBoxCloseRequest

Table 3: Defined URIs for the WS Addressing Action element

If this header element has not one of the values outlined, the message MUST be discarded and a fault MUST be generated.

Fault 2: **AddrWrongActionURI**
[Code] Sender
[Subcode] AddrWrongActionURI
[Reason] Invalid Action header URI value

/wsa:MessageID

R0180 - this mandatory element of type **xs:anyURI** MUST carry a unique message ID (UUID) according to IETF RFC "A Universally Unique Identifier (UUID) URN Namespace" [RFC4122]. An OSCI message MUST carry exactly one **/wsa:MessageID** SOAP header element.

/wsa:RelatesTo *

R0190 - these optional elements of type **xs:anyURI** MUST be included, if a message is to be seen as a response to preceding messages and in this case MUST carry the **wsa:MessageID** SOAP header entry of those messages. This is always the case for the network backchannel osci:Response and MsgBoxResponse. In case of asynchronous responses on Content Data level (carried in a new osci:Request) the values for these elements MUST be supplied by the responding Target Application. In case of an OSCIFetchedNotification (see chapter [8.3.3]), the value MUST be the one of the message currently being fetched out of a MsgBox instance.

/wsa:RelatesTo/@RelationshipType ?

This optional attribute of type **xs:anyURI** SHOULD be omitted. Following the semantics of [WSA], the implied value of this attribute is **"http://www.w3.org/2005/08/addressing/reply".**

6.2 Anonymous Access and use of WS MakeConnection

Endpoints MAY allow anonymous access. If this is the case, it MUST be exposed in a special policy assertion expressing X.509v3-Certificate token issued by public CSPs MUST be used for authentication.[7]

In a synchronous MEP, the response can be delivered in the http backchannel of the request. For this behaviour, WS-Addressing specifies the anonymous URI to be carried in the **/ReplyTo** EPR: **"http://www.w3.org/2005/08/addressing/anonymous".**

[7] An according policy template will be one part of the profilings addendum successively published from mid 2009 on

If the requesting Initiator has no OSCI endpoint available listening for messages (nor a MsgBox service instance), there exists to EPR the response to be delivered asynchronously can be targeted to.

For such responses to be delivered in an asynchronous way, the specification WS MakeConnection [WSMC] defines mechanisms to uniquely identify anonymous endpoints as well as making responses accessible for the Initiator in a response pulling manner. On the Recipient site special features have to be foreseen to hold responses until they are pulled. The fact a Recipient endpoint serves (and in this also requires) support of the MakeConnection protocol is indicated by a policy assertion as described in chapter [10.3].

OSCI implementations MAY support WS MakeConnection; no profilings apply here. Special attention should be taken here concerning the authentication requirements for anonymous Initiators and message security to prevent unauthorized message access.

The mechanisms of the WS MakeConnection protocol is seen to be useful for more or less sporadic OSCI based communication, where an initial registration process is not precondition to participate in an OSCI network. For such use cases, example policies will be made available be one part of the profilings addendum successively published from mid 2009 on.

7 Message Security, Authentication and Authorization

For the achievement of message confidentiality and integrity, the specification Web Services Security: SOAP Message Security 1.1 [WSS] is incorporated. The restrictions defined in the WS-I Basic Security Profile [WSI-BSP11] MUST strictly be applied by conformant implementations and MUST be matched by security policies defined for OSCI endpoints and service node instances.

Message protection mechanisms described here by means of encrypting and digitally signing only address scenarios, where potentially unsecured network connections are used for message exchange. Message exchange inside closed networks may be protected by other precautions out of band of this specification. But even for those scenarios it should be kept in mind that most of data and identity theft attacks are driven from inside companies, administrations and other institutions.

Every individual endpoint and service node SHOULD expose following information by means of WS Security Policies [WSSP] attached to their respective WSDL:

- Possible use of transport layer mechanisms (HTTP over SSL/TLS); if useable the profiling of [WSI-BSP11], chapter 3 "Transport Layer Mechanisms" is MUST be applied[8].
- If message layer mechanisms must be used: Which message parts have to be encrypted and signed as well as security token to be used for these purposes.
- What kind of token for authentication and authorization must be provided in a message.

Out of band agreement on theses issues between communication partners is accepted, too.

7.1 WS Security header block

No profiling going beyond WS-I Basic Security Profile [WSI-BSP11] is made to the layout and semantics of the **`/wsse:Security`** SOAP header block as defined in Web Services Security [WSS] except:

- Transport encryption and signing is achieved by means defined in [XMLDSIG] and [XENC] for which profilings are made in the following subchapters [7.2] and [7.3]. As defined by security policies, signature and/or encryption application to message parts is outlined in chapter [10].
- Supported security token types, outlined in chapter [7.4].

WS Security defines a Timestamp element for use in SOAP messages. OSCI places the following constraint on its use:

R0200 - A SOAP header **`/wsse:Security`** MUST contain exactly one element **`/wsu:Timestamp`**. This supersedes R3227 of [WSI-BSP11].[9]

7.2 XML Digital Signature

7.2.1 Restrictions to WS-I Basic Security Profiling

The profilings of [WSI-BSP11], chapter 8 "XML-Signature" is MUST be applied with following restrictions going beyond them:

R0300 - Transform algorithm **`"http://www.w3.org/2001/10/xml-exc-c14n#"`** is RECOMMENDED. This supersedes R5423 and R5412 of [WSI-BSP11] to clarify; this is the recommended algorithm of the list of algorithms which MUST be used following [WSI-BSP11].

[8] Applicable TLS/SSL versions and cyphersuites are defined here

[9] "MUST NOT contain more than one" is profiled by [WSI-BSP11]

R0310 - As the digest algorithm SHA-1 is seen to be week meanwhile, one of following digest method algorithms MUST be used:

Digest method algorithms
http://www.w3.org/2001/04/xmlenc#sha256
http://www.w3.org/2001/04/xmlenc#sha512
http://www.w3.org/2001/04/xmlenc#rsa-ripemd160

Table 4: Digest method: allowed algorithm identifiers

The use of SHA-256 (**http://www.w3.org/2001/04/xmlenc#sha256**) as digest method algorithm is RECOMMENDED. This supersedes R5420 of [WSI-BSP11][10].

R0320 - As the digest algorithm SHA-1 is seen to be week meanwhile, one of the signature method algorithms listed here MUST be used:

Asymmetric signature method algorithms
http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
http://www.w3.org/2001/04/xmldsig-more#rsa-sha512
http://www.w3.org/2001/04/xmldsig-more/rsa-ripemd160
Symmetric signature method algorithms
http://www.w3.org/2001/04/xmldsig-more#hmac-sha256
http://www.w3.org/2001/04/xmldsig-more#hmac-sha512

Table 5: Signature method: allowed algorithm identifiers

RECOMMENDED signature method algorithms are **http://www.w3.org/2001/04/xmldsig-more#rsa-sha256** and **http://www.w3.org/2001/04/xmldsig-more#hmac-sha256**. This supersedes R5421 of [WSI-BSP11][11].

NOTE on R0310, R0320: The URI-Values of the attributes **ds:SignatureMethod/@Algorithm** and **ds:DigestMethod/@Algorithm** are fixed to identifiers resulting from the actual list of strong hash algorithms published in [AlgCat]. One of the values outlined below MUST be choosen. *This enumeration is subject to future changes, in case of one of the algorithms must be seen to get weak*.

7.2.2 Format of XML Digital Signatures used for Documents

Besides securing message integrity, digital signatures are used in OSCI Transport to sign distinguished XML documents like policies and receipts, which in case of juridical conflicts must be usable as proof.

Here, the national signature laws and ordinances must be considered; in consequence profilings of relevant standards have already been derived as well as classification of applicability of cryptographic

[10] SHOULD is defined by [WSI-BSP11] for **http://www.w3.org/2000/09/xmldsig#sha1**

[11] SHOULD is defined by [WSI-BSP11] for signature method algorithms based on SHA-1

algorithms. This leads to a profiling of those XML Digital Signatures, which are applied on documents as advanced or qualified signatures using an appropriate X.509v3-Certificate.

In summary, following profiling of [XMLDSIG] and [XAdES] applies:

R0400 - The detached XML Signature format MUST be used and the signed content, if part of the message (child of SOAP envelope), be referenced by the local (fragment) URI mechanism as defined in [RFC2396]. Referencable fragments of message parts MUST carry an attribute of type **`xs:ID`**. The constraints of the XML 1.0 [XML 1.0] ID type MUST be met. The generation of unique ID attribute value MUST follow [RFC4122], this value SHOULD be concatenated to a preceding string **`"uuid:"`**.

R0410 - A **`ds:Signature`** element MUST contain at least one **`ds:Object`** child element to carry the signing time and a reference to the certificate used for signing. The format of this child element MUST conform to definitions given by [XAdES] with following restrictions applied here:

It MUST contain exactly on child element **`xades:QualifyingProperties`** including the mandatory child element **`xades:SignedProperties/xades:SignedSignatureProperties`** and an optional child element **`xades:UnsignedProperties`**, which is foreseen to carry a qualified timestamp over the signature itself in the child element **`xades:UnsignedSignatureProperties/xades:SignatureTimeStamp`**.

Child elements of **`xades:SignedSignatureProperties`** which MUST be present are **`xades:SigningTime`** and information about the certificate used for signing in **`xades:SigningCertificate`**.

R0420 - As consequence of R0300 and R0310, a **`ds:Signature`** element MUST contain at least two **`ds:Reference`** child elements for referencing at least one detached content and the elements in **`ds:Object`** to be included in the signature calculation.

R0430 - Exclusive canonicalization MUST be applied be used to address requirements resulting from scenarios where subdocuments are moved between contexts. The URI-Value of the attribute **`ds:CanonicalizationMethod/@Algorithm`** is fixed to **`"http://www.w3.org/2001/10/xml-exc-c14n#"`**.[12]

R0440 - Signatures are only applicable on base of X.509v3-Certificates which MUST conform to [COMPKI]. The child elements **`ds:RetrievalMethod`** and **`ds:X509Data`** of **`ds:KeyInfo`** MUST be present. All other choices according to [XMLDSIG] for **`ds:KeyInfo`** MUST NOT be present. In consequence, the attribute **`ds:RetrievalMethod/@Type`** MUST carry a value of **`"http://www.w3.org/2000/09/xmldsig/X509Data"`**.

R0450 - The child elements **`ds:X509IssuerSerial`** and **`ds:X509Certificate`** of **`ds:X509Data`** MUST be present; the child element **`ds:X509CRL`** SHOULD NOT be present to avoid significant data overload of signature elements to be expected in case of including CRLs. All other choices according to [XMLDSIG] for **`ds:X509CRL`** and **`ds:X509SKI`** MUST NOT be present.

Details profiling and restrictions are defined by the following normative outline:

```
<ds:Signature Id="xs:ID">
  <ds:SignedInfo Id="xs:ID" ?>
    <ds:CanonicalizationMethod
       Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
    </ds:CanonicalizationMethod>
```

[12] See also: R5404 of [WSI-BSP11]

```
570
571       <ds:SignatureMethod Algorithm=
572             http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 |
573             http://www.w3.org/2001/04/xmldsig-more#rsa-sha512 |
574             http://www.w3.org/2001/04/xmldsig-more/rsa-ripemd160
575       </ds:SignatureMethod>
576
577      <ds:Reference Id="xs:ID" ?
578         Type="http://uri.etsi.org/011903/v1.1.1/#SignedProperties"
579         URI="xs:anyURI">
580      <ds:Transforms/> ?
581        <ds:DigestMethod Algorithm=
582           http://www.w3.org/2001/04/xmlenc#sha256 |
583           http://www.w3.org/2001/04/xmlenc#sha512 |
584           http://www.w3.org/2001/04/xmlenc#rsa-ripemd160
585        </ds:DigestMethod>
586     <ds:DigestValue> xs:base64Binary </DigestValue>
587       <ds:Reference>
588
589    (<ds:Reference Id="xs:ID" ?
590        Type="xs:anyURI"
591        URI="xs:anyURI">
592      <ds:Transforms/> ?
593      <ds:DigestMethod Algorithm=
594            http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 |
595            http://www.w3.org/2001/04/xmldsig-more#rsa-sha512 |
596            http://www.w3.org/2001/04/xmldsig-more/rsa-ripemd160
597         </ds:DigestMethod>
598      <ds:DigestValue> xs:base64Binary </DigestValue>
599     </ds:Reference> ) +
600
601    </ds:SignedInfo>
602
603    <ds:SignatureValue Id="xs:ID" ?> xs:base64Binary </ds:SignatureValue>
604
605    <ds:KeyInfo Id="xs:ID" ?>
606     <ds:RetrievalMethod
607           Type="http://www.w3.org/2000/09/xmldsig/X509Data"/>
608     <ds:X509Data>
609       <ds:X509IssuerSerial>
610         <ds:X509IssuerName> xs:string </ds:X509IssuerName>
611         <ds:X509SerialNumber> xs:integer </ds:X509SerialNumber>
612       </ds:X509IssuerSerial>
613       <ds:X509Certificate> xs:base64Binary> </ds:X509Certificate>
614       <ds:X509CRL/> ?
615     </ds:X509Data>
616    </ds:KeyInfo>
617
618  <ds:Object Id="xs:ID">
619     <xades:QualifyingProperties Target="...">
620       <xades:SignedProperties>
621         <xades:SignedSignatureProperties Id="xs:ID">
622           <xades:SigningTime> xs:dateTime </xades:SigningTime>
623           <xades:SigningCertificate>
624             <xades:Cert>
625               <xades:CertDigest>
626                  <ds:DigestMethod> Algorithm=
627                        http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 |
628                        http://www.w3.org/2001/04/xmldsig-more#rsa-sha512 |
```

```
                    http://www.w3.org/2001/04/xmldsig-more/rsa-ripemd160
            </ds:DigestMethod>
            <ds:DigestValue> xs:base64Binary </DigestValue>
          </xades:CertDigest>
          <xades:IssuerSerial>
                     <ds:X509IssuerName> xs:string </ds:X509IssuerName>
                     <ds:X509SerialNumber>
                        xs:integer
                     </ds:X509SerialNumber>
          </xades:IssuerSerial>
        </xades:Cert>
      </xades:SigningCertificate>
    </xades:SignedSignatureProperties>
  </xades:SignedProperties>

 ( <xades:UnsignedProperties Id="xs:ID" ?>
    <xades:UnsignedSignatureProperties id="xs:id" ?>
     <xades:SignatureTimeStamp id="xs:ID" ?>
      ( <ds:CanocalizationMethod
       Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
      </ds:CanocalizationMethod> ) ?
      <xades:EncapsulatedTimeStamp>
         Id="xs:ID" ? Encoding="xs:ID" ?>
       xs:base64Binary
      </xades:EncapsulatedTimeStamp>
     </xades:SignatureTimeStamp>
    </xades:UnsignedSignatureProperties>
  </xades:UnsignedProperties> ) ?

 </xades:QualifyingProperties>
</ds:Object>
<ds:Object Id="xs:Id" ?/> ?
</ds:Signature>
```

The outline above shows mandatory and optional elements and their cardinality restrictions. For a detailed description of elements and attributes in the outline above, see [XMLDSIG] and [XAdES].

For illustration, an example is given for an instance of such a signature element in [0].

7.3 XML Encryption

In general, the profilings of [WSI-BSP11], chapter 9 "XML Encryption" is MUST be applied. If encryption is applied, the SOAP envelope, header, or body elements MUST NOT be encrypted. Encrypting these elements would break the SOAP processing model and is therefore prohibited (see R5607 of [WSI-BSP11]).

Restrictions going beyond [WSI-BSP11] are defined in the following subchapters.

7.3.1 End-to-end Encryption of Content Data

Following general rules apply in addition to those presented in chapter [7.3.2]:

R0400 - A SOAP message body block MUST be encrypted for the intended Ultimate Recipient following [XENC] using the public key of his X.509v3 encryption certificate.

R0410 - A hybrid encryption algorithm MUST be applied: First a random session key is generated for a symmetric encryption algorithm. Using this key, the SOAP body blocks are encrypted. In a second step the session key is encrypted with the public encryption key of the Ultimate Recipient. The encrypted data and the encrypted session key build up the resulting SOAP body block of the message.

R0420 - It MUST be ensured that not the same session key is used for data that are directed to different Ultimate Recipients.

7.3.2 Encryption Cyphersuite Restrictions

R0500 - One of following symmetric block encryption algorithms MUST be used:

Encryption Algorithm	Algorithm Identifier
Two-Key-Triple-DES	**http://www.w3.org/2001/04/xmlenc#tripledes-cbc**
AES-128	**http://www.w3.org/2001/04/xmlenc#aes128-cbc**
AES-192	**http://www.w3.org/2001/04/xmlenc#aes192-cbc**
AES-256	**http://www.w3.org/2001/04/xmlenc#aes256-cbc**

Table 6: Symmetric encryption algorithms

R0510 - Encryption of symmetric keys MUST be performed by means of RSAES-PKCS1-v1_5 [PKCS#1]. The value of **xenc:EncryptionMethod** MUST be

"http://www.w3.org/2001/04/xmlenc#rsa-1_5"

R0520 - The modulus length of a RSA key pair has to be at least 2048 bit.

7.4 Security Token Types

To be extensible, the WS-Security specification has not bound to specific security token types. For this version of OSCI Transport, token types outlined in following table MAY be used for authentication, message signature and encryption operations. Profilings of those token types have been specified by the OASIS Web Services Security Technical Committee.

Security Token Type	Support	Value of **wsse:BinarySecurityToken/@ValueType** and **wsse:SecurityTokenReference /wsse:KeyIdentifier/@ValueType**	Profiling Reference
SAMLV2.0	MUST	**http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0**	[WSSSAML]
X.509v3-Certificate	MUST	**http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3**	[WSSX509]
Kerberos	MAY	**http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#GSS_Kerberosv5_AP_REQ**	[WSSKERB]
Username	MAY	Defined in WS-Security as **wsse:UsernameToken**	[WSSUSER]

Table 7: Security token types – support requirements

R0600 - SAMLV20-Token MUST be used for authentication and message security within Trust Domains as well as for cross domain message exchange – except R0610 applies.

If access of anonymous Initiators shall be supported, Public Key Infrastructure MUST be used applying X.509v3-Certificates:

R0610 - X.509v3-Certificate token issued by CAs MUST be used for authentication and message security for scenarios allowing anonymous access. Validity of used certificates MUST be verifiable by means of OCSP, LDAP or CRL.

The node a message is targeted to MUST verify the certificate validity; in case a value other than valid at time of usage is stated, the message MUST be discarded and a fault MUST be generated.

Fault 3: **AuthnCertNotValid**
[Code] Sender
[Subcode] AuthnCertNotValid
[Reason] Authentication certificate not stated to be valid

More information about the certificate validation results SHOULD be provided in the fault [Details] property in this case. It is strongly RECOMMENDED to log such faults to be able to detect possible security violation attacks.

R0620 - X.509v3-Certificates used for authentication MUST have set the key usage extension set to “digitalSignature". If the “nonRepudiation" key usage is set, these certificates MUST not be used for authentication.[13]

Context conformant usage of certificates and their validity SHOULD be controlled by STS respective message initiating instances to avoid subsequent violations of this requirement. The node a message is targeted to MUST verify conformance this requirement; in case of wrong key usage set, the message MUST be discarded and a fault MUST be generated.

Fault 4: **AuthnCertInvalidKeyUsage**
[Code] Sender
[Subcode] AuthnCertInvalidKeyUsage
[Reason] Certificate not permitted for authentication

Token of type Username and Kerberos MAY be used for authentication and securing messages inside closed communication domains, where security and trust is given be means out of band of this specification.

7.5 Use of WS-Trust and SAML Token

In general, means of WS-Trust[14] SHOULD be used where all communication partners of a Trust Domain are registered at an IdP, having a STS available for issuing SAML-Token.

R0630 - Each access to an endpoint MUST be authorized by a STS instance of the endpoints Trust Domain. A STS MUST be able to confirm the Requestors identity on base of presented credentials.

For a given Trust Domain, the definition of a standard security policy and SAM Token layout is RECOMMENDED, which can basically be used for message exchange inside this domain. If certain services have special authentication and/or authorization requirements, this can be propagated in according security policies bound to these services respective endpoints.

[13] The signature used for authentication must not be confused with the legal declaration of intend given by a (qualified) digital signature.

[14] An overview for use of WS-Trust and SAML-Token is given in chapter [**Fehler! Verweisquelle konnte nicht gefunden werden.**].

7.5.1 Authentication Strongness

Access authorization at least is given by the assurance of a certain level of authentication of the STR. Trustworthiness of the STR identity confirmation thru an STS is given by the strongness of following two processes:

- Initial registration of an endpoint at his IdP – organizational rules that applied for the degree of trustworthiness initial subject identification
- Mechanisms used for authentication at the time of requesting identity confirmation from the STS to match claimed and conformed identity.

[SAML2] and [SAMLAC] specify an authentication statement **`saml:AuthnStatement`** to carry such information. Differentiated authentication context details may be included herein. To simplify processing and interoperability, following ascending levels for strongness of registration and authentication are defined[15]:

- **`urn:de:egov:names:fim:1.0:securitylevel:normal`**
- **`urn:de:egov:names:fim:1.0:securitylevel:high`**
- **`urn:de:egov:names:fim:1.0:securitylevel:veryhigh`**

Each level matches operational rules which must be defined, published and continuously maintained by appropriate institutions, i.e. government agencies concerned to data protection.[16]

[SAFE] defines extensions to the SAML authentication context element to carry the levels of registration and authentication as follows:

```
<samlac:Extension>
  <fimac:SecurityLevel>
    <fimac:Authentication>
       urn:de:egov:names:fim:1.0:securitylevel:normal |
       urn:de:egov:names:fim:1.0:securitylevel:high |
       urn:de:egov:names:fim:1.0:securitylevel:veryhigh |
    </fimac:Authentication> ?
    <fimac:Registration>
       urn:de:egov:names:fim:1.0:securitylevel:normal |
       urn:de:egov:names:fim:1.0:securitylevel:high |
       urn:de:egov:names:fim:1.0:securitylevel:veryhigh |
    </fimac:Registration> ?
  </fimac:SecurityLevel> ?
</samlac:Extension> ?
```

This outline is preliminary to be seen as normative.

`/samlac:Extension ?`

Optional container carrying the extension; to be included in a SAML assertion in the **`samlac:AuthenticationContextDeclaration`** element.

…**`/fimac:SecurityLevel ?`**

Optional container carrying the detail elements.

…**`/fimac:SecurityLevel/fimac:Authentication ?`**

Optional authentication level statement of type restriction to **`xs:anyURI`**; if present, the URI value MUST be one of the enumerations listed above.

…**`/fimac:SecurityLevel/fimac:Registration ?`**

[15] Preliminary URIs proposed by the SAFE-Project; subject to standardization activities by German administration

[16] Definition of such rules can not be a matter of this specification. An example for a level “veryhigh” could be a registration data confirmation on base of presenting Id Cards and subsequent authentication using authentication certificates issued by accredited CAs.

Optional registration strongness statement of type restriction to **`xs:anyURI`**; if present, the URI value MUST be one of the enumerations listed above.

If a SAML token of a message addressed to an endpoint does not match the minimal security level requirements of this endpoint, the message MUST be discarded and a fault MUST be generated.

Fault 5: **AuthnSecurityLevelInsufficient**	
[Code]	Sender
[Subcode]	AuthnSecurityLevelInsufficient
[Reason]	Insufficient strongness of authentication or registration

Detailed information on the security level requirements SHOULD be provided in the fault [Details] property in this case.

To facilitate the acquisition of an appropriate SAML token for the Initiator, endpoints SHOULD describe there requirements on authentication strongness by means of WS-Policy as outlined in chapter [].

7.5.2 WS-Trust Messages

Conformant OSCI Gateway implementations MUST support the SOAP message types and bindings defined by WS-Trust:

- Issue
- Validate
- Cancel.

The WS-Trust Reniew-Binding SHOULD be supported for convenience; this functionality is supplied by most STS-Implementions.

For clarification, an overview is given in following subchapters to the constituents of these message types. For the exact definition of the according XML Infoset see [WST]; the present document concentrates on restrictions to be applied by OSCI conformant implementations and a few hints.

7.5.2.1 Request Security Token (RST)

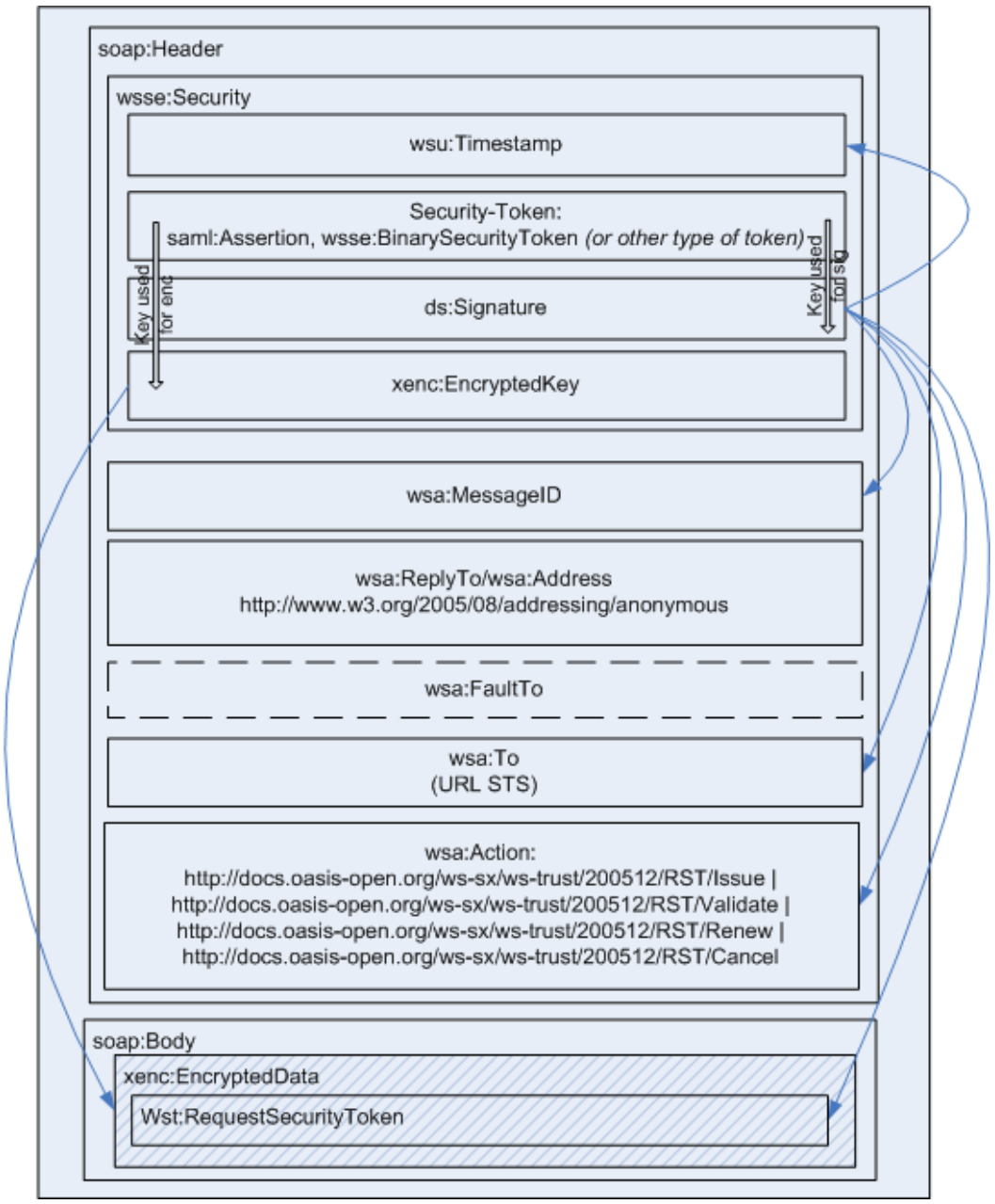


Figure 1: Request Security Token Message

SOAP header blocks:

`/wsse:Security`

This header block MUST be present, carrying message protection data and Initiator authentication information according the security policy of the STS the RST message is targeted to.

`/wsse:Security/wsu:Timestamp`

According to R0200, this header block MUST be present.

`/wsse:Security/[Security-Token]`

Security tokens MUST be used for signing and encrypting message parts. **`ds:KeyInfo`** elements of subsequent **`ds:Signature`** or **`xenc:EncryptedKey`** elements MAY point to security tokens carried here.

[Table 7] lists the security token types which MUST or MAY be supported.

Security tokens MUST be embedded or referenced. Referenced tokens MUST be dereferencable by the targeted STS.

The Requestors security token MUST be used for signing the above marked message parts.

`/wsse:Security/ds:Signature`

A signature containing **`ds:Reference`** elements to all message parts marked above to be included in the signature.

`/wsse:Security/xenc:EncryptedKey`

The RST contained in the SOAP body block MUST be encrypted for the targeted STS. This is a symmetric key which MUST be encrypted with the public key of the STS X.509v3 encryption certificate. Rules outlined in chapter [7.3] apply. It is assumed, that the STS encryptions certificate is made available to all endpoints inside the STS Trust Domain out of band of this specification.

`/wsa:*`

All WS-Addressing headers MUST (if in continuous blocks) /MAY (if in dashed blocks) be supplied by the Requestor.

`/wsa:Action`

Depending on the type of WS-Trust request, one of the URIs outlined above MUST be supplied. This URI MUST be adequate to the respective body block content.

The SOAP body block MUST conform to the definitions of WS-Trust, whereby following restrictions and recommendations apply for the WS-Trust Issue request type.

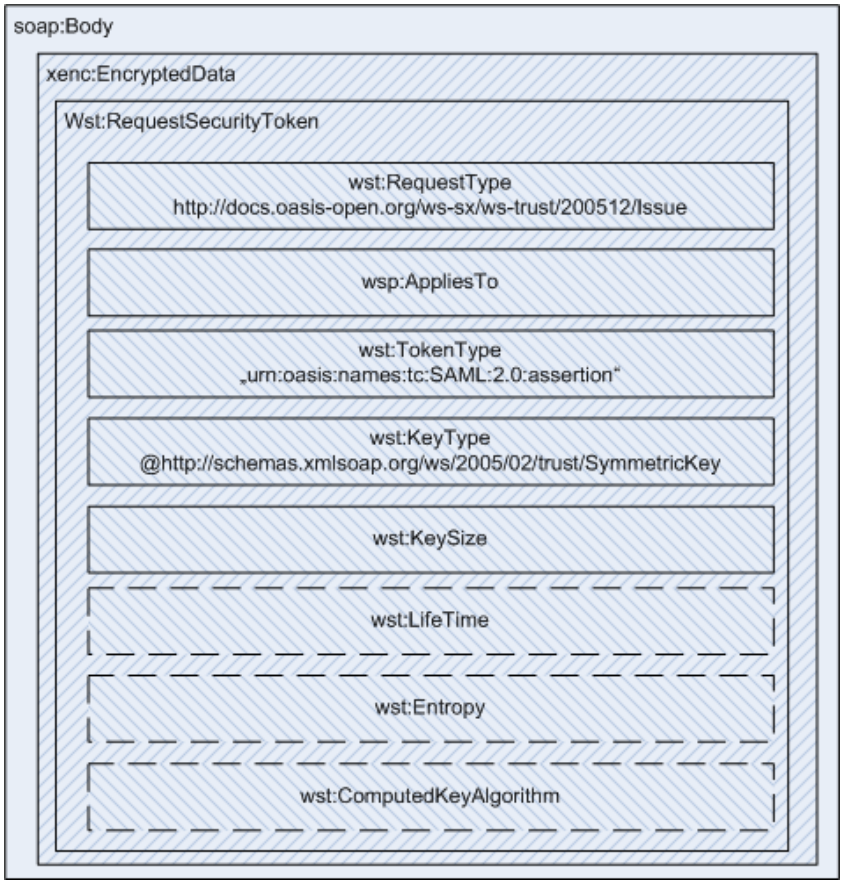


Figure 2: Request Security Token, Body for Issue Request

841 **/wsp:AppliesTo**

842 This element MUST be present; the value assigns a domain expression for the desired
843 application scope of the SAML-Token.

844 NOTE: For easy of message exchange inside a Trust Domain, it is RECOMMENDED to
845 choose an expression (i.e. URL pattern) accepted at least by a MsgBox instance for all
846 Recipients nodes using this MsgBox instance. This leverages the burden and overhead,
847 which would be given by a **/wsp:AppliesTo** value assignment to a concrete Recipient
848 EPR.

849 **/wst:TokenType**

850 R0700: This element MUST be present; the value is restricted to SAML V2.0 assertion
851 type:

852 **urn:oasis:names:tc:SAML:2.0:assertion**

853 **/wst:KeyType**

854 R0710: This element MUST be present; the value is restricted to:

855 **http://docs.oasis-open.org/ws-sx/ws-trust/200512/SymmetricKey**

856 **/wst:KeySize**

857 R0720: This element MUST be present; the key size MUST be greater or equal 256 Bit.

858 Use and values of elements marked optional are subject to used STS instance specific policies.
859 Recommendations will we given as part of the amendments to be worked out for this specification in
860 2009 ff.

7.5.2.2 Request Security Token Response (RSTR)

The SOAP header resembles the one of the RST message:

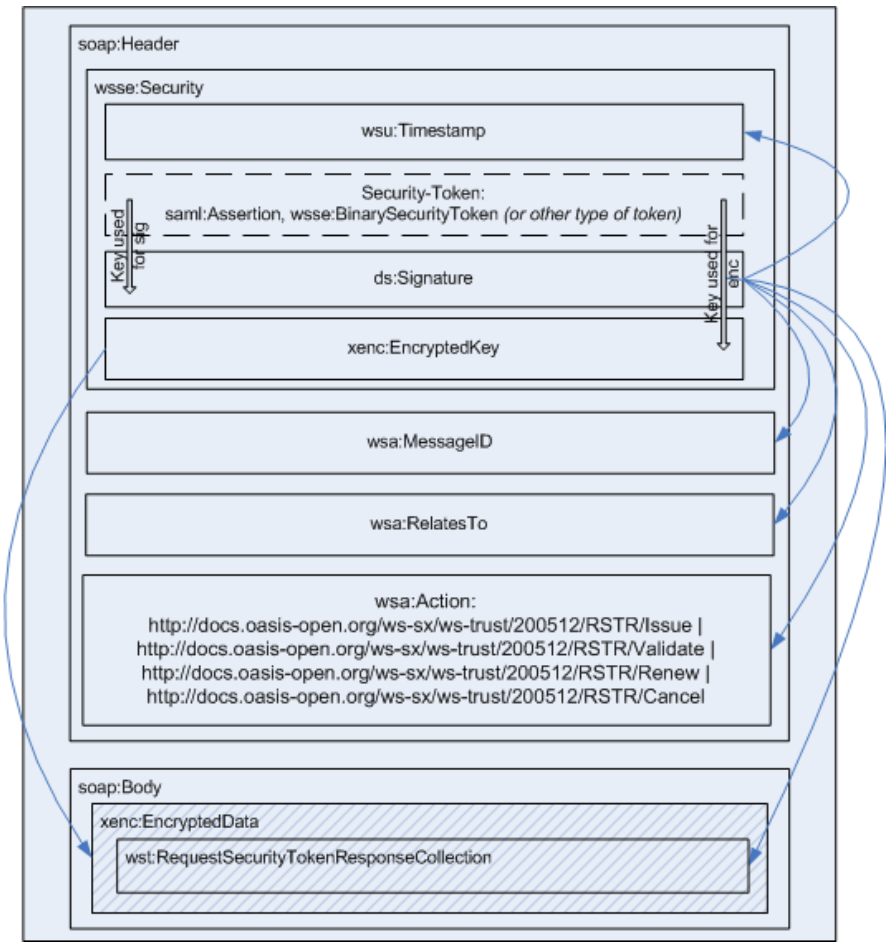


Figure 3: Request Security Token Response Message

Differences to the RST message:

`/wsse:Security/xenc:EncryptedKey`

The RSTRC contained in the SOAP body block MUST be encrypted for the token Requestor. This is a symmetric key which MUST be encrypted with the public key of the Requestors X.509v3 encryption certificate. Rules outlined in chapter [7.3] apply.

`/wsa:*`

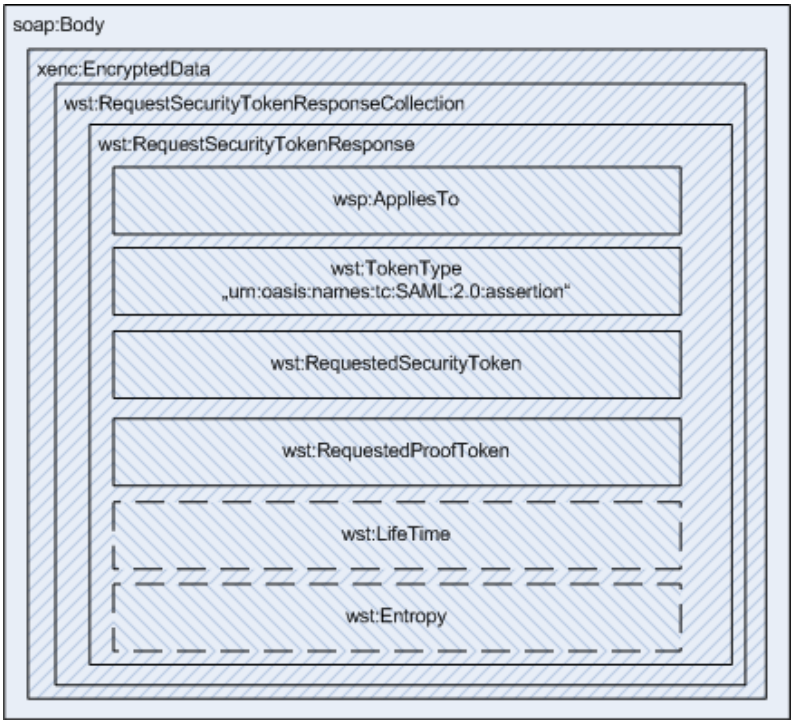
All WS-Addressing headers MUST (if in continuous blocks) /MAY (if in dashed blocks) be supplied by the STS.

`/wsa:Action`

Depending on the type of WS-Trust response, one of the URIs outlined above MUST be supplied. This URI MUST be adequate to the respective body block content.

The decrypted SOAP body block MUST conform to the definitions of WS-Trust. No restrictions or profilings apply.

878 The SOAP body block MUST conform to the definitions of WS-Trust:



879

880 Figure 4: Request Security Token, Body for Issue Response

881 Short description of the constituents of **`/wst:RequestSecurityTokenResponse`**, which is always
882 wrapped by a **`/wst:RequestSecurityTokenResponseCollection`** (see [WST] for details):

883 **`/wsp:AppliesTo`**

884 Carries the value assignment for the desired application scope of the requested security
885 token – copied from the according request element.

886 **`/wst:TokenType`**

887 Carries the token type, which MUST be the one of the according request element.

888 **`/wst:RequestedSecurityToken`**

889 Carries the requested SAML-Token, including a symmetric key encrypted for the endpoint
890 at which the SAML-Token is needed for authentication purposes. Details explained in
891 chapter [7.5.3].

892 **`/wst:RequestedProofToken`**

893 Carries information enabling the Requestor to deduce the symmetric key. In case the key
894 was generated by the STS solely, this is the key itself.

895 In case computed of two entropy values, this is the algorithm and the element

896 **`/wst:Entropy ?`**

897 MUST be present carrying the entropy value used by the STS for key computation.

898 **`/wst:LifeTime ?`**

899 Optional element carrying the validity duration period of this RSTR; SHOULD be
900 recognized by the Requestor and processed according to his needs to avoid using
901 security tokens being/getting invalid.

7.5.3 Issued SAML-Token Details

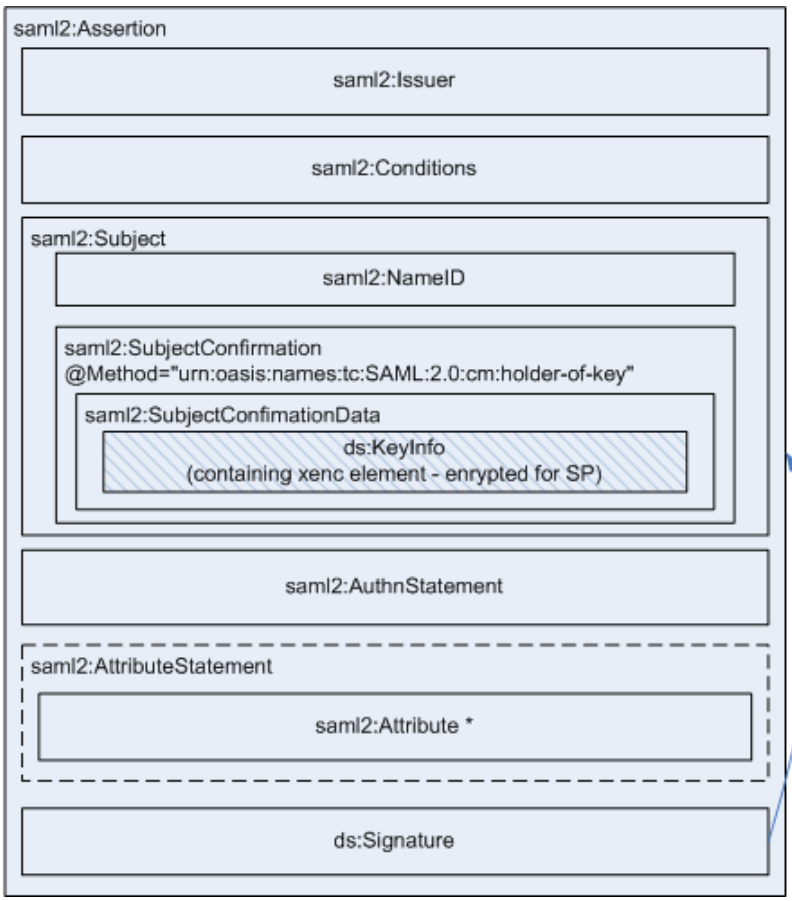


Figure 5: SAML 2.0 Assertion constituents

Short description of the constituents of a **`/saml2:Assertion`**, for XML Infoset details see [SAML2] and [SAMLAC]. The concrete token request requirements and layout of issued token at least has to be matched with the capabilities of the used STS instances. For implementations to be operated in context of the German administration it is strongly RECOMMENDED to follow requirements and recommendations given by the concept [SAFE].

`/saml2:Issuer`

Attributes of the STS issuing this assertion; for details see **`saml2:NameIDType`**

`/saml2:Conditions`

R0730: Detailed validity conditions element MUST be present; for details see **`saml2:ConditionsType.`** MUST at least outline the validity period attributes **`NotBefore`**, **`NotOnOrAfter`**.

`/saml2:Subject`

R0740: Presence of this element is REQUIRED. The subelements of this container provide STR identification details.

`/saml2:Subject/saml2:NameID`

Attributes of the STR; for details see **`saml2:NameIDType`**. It MUST at least contain a unique string identifying the STR.

`/saml2:Subject/saml2:SubjectConfirmation`

This container exposes STS information for the SP enabling it to assure the SR is the one stated in **`/saml2:NameID`** and authorized to use this token.

925 **/saml2:Subject/saml2:SubjectConfirmation/@Method**

926 R0750: Attribute outlining the confirmation method; MUST be the "holder of key"
927 confirmation method.

928 **/saml2:Subject/saml2:SubjectConfirmation/saml12:SubjectConfirmationData**

929 R0760: Presence of this element is REQUIRED; it exposes STS information for the SP
930 enabling it to assure the SR is the one owning key for this SAML assertion.

931 **/saml2:Subject/saml2:SubjectConfirmation/saml12:SubjectConfirmationData/ds:**
932 **key**

933 R0770: This element MUST carry the key in a **xenc:EncryptedKey** element. The key
934 MUST be encrypted for the SP using the public key of its X.509v3 encryption certificate,
935 which for this purpose MUST be made available to the STS.

936 NOTE on the endpoint encryption certificate the SAML token is targeted to:

937 The access to this certificate through the token issuing STS is of band of this specification;
938 this is a matter of Trust Domain policies and an implementation issue which MUST have
939 no effect on interoperability. No standardized mechanisms are foreseen by WS-Trust, to
940 include a certificate in a RST message for the purpose of key encryption for the SP. It is
941 strongly RECOMMENDED, to relate the **/wsp:AppliesTo** request value (which might
942 be a pattern, too – see RST body description in chapter [7.5.2.1]) to this encryption
943 certificate.

944 **/saml2:AuthnStatement**

945 R0780: Presence of this element is REQUIRED.

946 It MUST contain an element **/saml2:AuthnContext** with an attribute **@AuthnInstant**
947 outlining the time instant the authentication took place.

948 **/saml2:AuthnContext** MUST contain an element **/saml2:AuthnContextClassRef**
949 outlining the authentication method used by the SR.[17]

950 **/saml2:AuthnContext** MUST further contain an element
951 **/saml2:AuthnContextDecl** carrying the extensions for authentication strongness as
952 defined in chapter [7.5.1].

953 **/saml2:AttributeStatement ?**

954 Usage of attribute statements of type **saml12:AttributeType** is RECOMMENDED. In
955 many scenarios subject attributes like affiliation to certain groups or roles are used for the
956 assignment detailed rights, functions and data access. Hence attributes are specific to
957 application scenarios, their names, values and semantics are subject to the overall design
958 of a domain information model, which is not addressed by this specification.[18]

959 **/ds:Signature**

960 The issuing STS has to sign the whole SAML-Token.

[17] See [SAMLAC] and [SAFE] for details; i.e. a X509v3 certificate from a smartcard was used for authentication, the value would be **urn:oasis:names:tc:2.0:ac:classes:SmartcardPKI**

[18] Suggestions for use in German eGovernment, especial eJustice, are made in [SAFE]

If a SAML token does not match one or more of the formal requirements 0730-0780, the token consuming node MUST generate a fault and discard the message.

Fault 6: **AuthnTokenFormalMismatch**	
[Code]	Sender
[Subcode]	AuthnTokenFormalMismatch
[Reason]	Authentication token present does not match formal requirements.

More information MAY be given in the fault [Details] property, but care should be taken to introduce security vulnerabilities by providing too detailed information.

7.5.4 Authentication for Foreign Domain Access

To authenticate and authorize access to foreign TD endpoints, these endpoints MUST be able to validate the SAML-Token contained in the message. The specification WS-Federation 1.1 ([WSF], chapter 2.4) outlines several possible trust topologies; for simplification, two of those described below are selected to be applicable for this version of the OSCI specification.

A new version 1.2 of WS-Federation is about to be approved by the OASIS WSFED Technical Committee while publishing the here presented version of OSCI Transport. WS-Federation 1.2 will be incorporated in a follow-up of OSCI Transport. So far, the WS Fedaration metadata model is not yet been taken in account for usage in OSCI 2.0 based infrastructures.

Precondition for cross domain message exchange is an established trust relationship between the Initiators STS and the one of the foreign TD. This i.e. can be achieved by trust in the STS signature using its signing certificate as a trust anchor.

One useable trust model is, a SAML-Token issued by the foreign STS must be aquired for accessing endpoints in this TD. Authentication at foreign STS in this case is obtained on base of presenting the SAML-Token of the Initiators STS in the according RST issue message. Depending on policies in effect, this SAML-Token may be replaced or cross-certified by applying a new signature. The SAML-Token key MUST be encrypted for the endpoint access is intended for. At the endpoint accessed, SAML-Token validation can be done on base of the signature of the foreign TD STS.

In the second trust model, the SAML-Token issued by the Initiator's STS directly is used for access authentication. In this case, the foreign endpoint points a RST validate message to his trusted STS for validatind the foreign SAML-Token – what there again is done on base of SAML-Token signature, which must be trestud by the validating STS. Again, the SAML-Token key MUST be encrypted for the endpoint access is intended for.

Details of the required SAML Token including claims and the issuing STS address as well as public key of this STS encryption certificate SHOULD be exposed by the endpoint WSDL. Apart, means of WS-Trust as already outlined in the chapters above apply.

7.5.5 SAML-Token for Receipt- /Notification Delivery

Requested receipts and notifications which cannot be delivered in the network backchannel of a request message MUST be delivered using an independent request message asynchronously to the EPR outlined in the receipt/notification request – which in general SHOULD be the Initiators MsgBox. As – like for all messages - delivery of receipts/notifications to this EPR requires authentication and authorization, an according SAML-Token SHOULD be forwarded to the receipt/notification generating node together with the request for it. This mechanism disburdens these nodes from the acquisition of an extra SAML-Token to authenticate receipt/notification delivery.

This type of SAML-Token - referred to as "**OneTimeToken**" - is valid only for "one time use" of receipt/notification delivery and bound to the **`wsa:MessageID`** of the message to be receipted/notified. Following rules apply:

1. It MUST be requested from the Initiators's STS.
2. The according RST message MUST contain the **`wsa:MessageID`** and the address of the receipting/notifying node (**`wsp:AppliesTo`**) as claims.
3. The symmetric key of the issued SAML-Token MUST be encrypted for the endpoint outlined in the element …**`/wsa:ReplyTo`** of the receipt/notification demand; the **`wst:RequestedProofToken`** in this case MUST be encrypted for receipting/notifying node (for use in step 6. ahead)
4. The issuing STS MUST retain this OneTimeToken for later use and mark it as "unused".
5. The RSTR message returned by the STS MUST be included as separate SOAP header block in the request message.
6. The receipting/notifying node has to use the OneTimeToken included in this RSTR as SAML-Token for the message the receipt/notification is delivered with. Transport signature and encryption MUST be generated on base of the symmetric key contained in the **`wst:RequestedProofToken`**.

Steps to be done by the node this message is targeted to:

7. Decryption of the OneTimeToken's symmetric key.
8. Validation of the signature of the OneTimeToken – the symmetric key MUST be the same the receipting/notifying node used for the transport signature.
9. Validation of the signature of the issuing STS and RST-Validate message containing the OneTimeToken to the STS.
10. If at the issuing STS this OneTimeToken is still marked as "unsed", the token is is valid.
11. If RSTR in validate-request signals valid: Acceptance of the message containing the receipt/notification.
12. Message accpeting node MUST generate a RST/cancel message to the STS to invalidate this OneTimeToken; STS SHOULD discard this token.

Following diagrams illustrate the RST and RSTR for the OneTimeToken, for concrete XML Infoset descriptions see WS-Trust and SAML specifications.

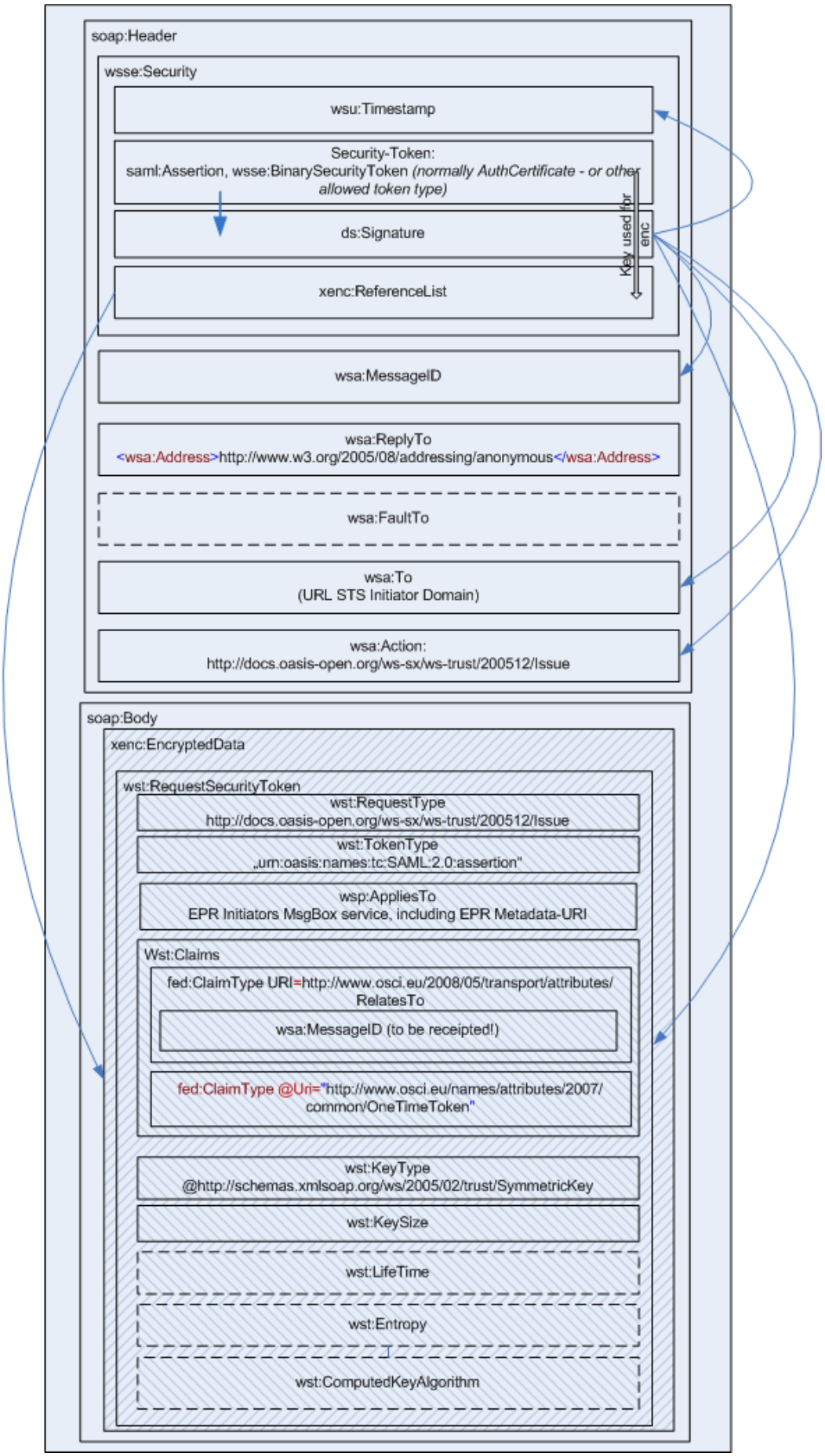


Figure 6: RST for OneTimeToken

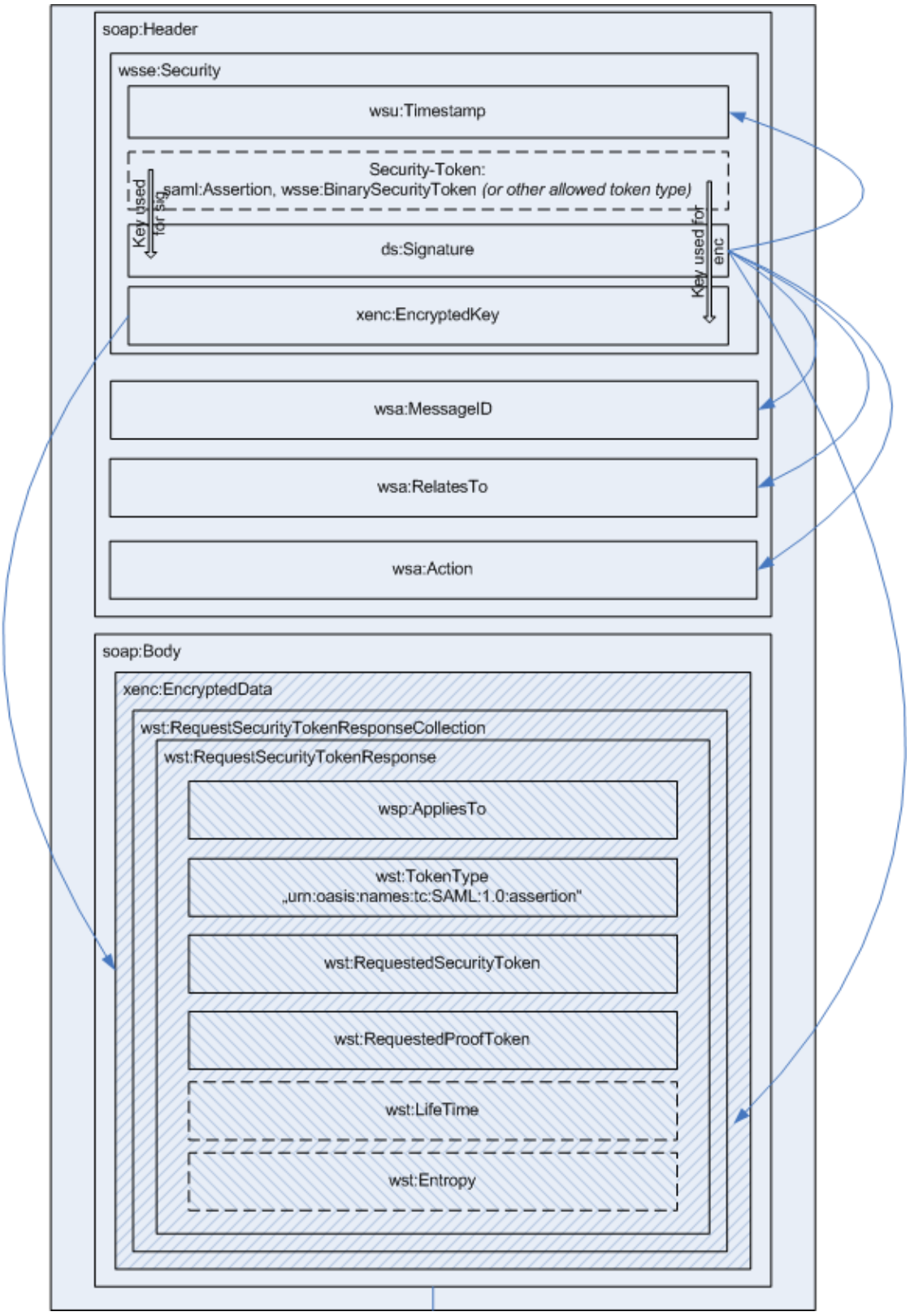


Figure 7: RSTR for OneTimeToken

8 OSCI specific Extensions

8.1 Message Flow Time Stamping

For sake of traceability of message flow time instants and delivery status, every message of type osci:Request MAY contain following SOAP header block, which child elements are provided depending on the nodes passed in the message flow.

```
<osci:MsgTimeStamps wsu:Id="..." ? >
  <osci:ObsoleteAfter> xs:date </osci:ObsoleteAfter> ?
  <osci:Delivery> xs:dateTime </osci:Delivery> ?
  <osci:InitialFetched> xs:dateTime </osci:InitialFetch> ?
  <osci:Reception> xs:dateTime </osci:Reception> ?
</osci:MsgTimeStamps>
```

Description of elements and attributes in the schema overview above:

`/osci:MsgTimeStamps`

This complex element is the container for various optional timestamp elements. It MUST be created from the first node on the message flow which applies one or more sub-elements.

`/osci:MsgTimeStamps/@wsu:Id`

For ease of referencing this SOAP header block from WS Security SOAP header elements, this attribute of type **`wsu:Id`** SHOULD be provided.

`/osci:MsgTimeStamps/osci:ObsoleteAfter ?`

This element of type **`xs:date`** MAY be provided by an Initiator to denote the date after which a message is to be seen as obsolete for delivery and/or consumption. It MUST NOT be provided or changed by other nodes on the message path.

If and how this information is handled by this endpoint this message is targeted to if outlined in the policy of this endpoint; see chapter [10.2.2] for details.

`/osci:MsgTimeStamps/osci:Delivery ?`

This element of type **`xs:dateTime`** MUST be provided by a MsgBox node when accepting an incoming message and MUST to be set to the value of the actual MsgBox server time.

It MUST NOT be provided or changed by other nodes on the message path.

`/osci:MsgTimeStamps/osci:InitialFetched ?`

This element of type **`xs:dateTime`** MUST be provided by a MsgBox node with to the value of the actual MsgBox server time when an authorized Recipient initially pulls the message from his MsgBox instance.commits the successful initial reception of this message. This SHOULD be done by a Recipient after the first successful pulling of the message from his MsgBox.

It MUST NOT be provided or changed by other nodes on the message path. Pull processes on the same message following a first confirmed one, this element MUST NOT be updated.

`/osci:MsgTimeStamps/osci:Reception ?`

This element of type **`xs:dateTime`** MAY be set by a Recipient to his actual server time when successfully accepting an incoming message, but it should be considered that the

signature is invalidated which was applied over SOAP header and body elements by the message issuing instance.

It MUST be set by a MsgBox node to his actual server time when the recipient commits the reception of a message thri a MsgBoxGetNextRequest or MsgBoxCloceRequest.

It MUST NOT be provided or changed on the message path by other nodes than described here.

8.2 Accessing message boxes

Following chapters define how to access MsgBox services for searching and pulling out messages as well as how to gain status lists describing content of message boxes. Statuses of those requests are delivered in the SOAP header block of the correlating responses, while the pulled messages respective status lists are delivered in the SOAP body block.

We describe the requests first, followed by the respective responses and additional messages to model "get next", "commit" and "close" semantics for iterative MsgBox access sequences.

8.2.1 MsgBoxFetchRequest

To request a message from an endpoint, a requestor MUST send a MsgBoxFetchRequest message to his MsgBox instance endpoint.

The normative outline for a MsgBoxFetchRequest request is:

```
<s12:Envelope ...>
 <s12:Header ...>
  ...
  <wsa:Action>
http://www.osci.eu/ws/2008/05/transport/urn/messageTypes/MsgBoxFetchRequest
  </wsa:Action>
  <wsa:MessageID>xs:anyURI</wsa:MessageID>
  <wsa:ReplyTo>wsa:EndpointReference</wsa:ReplyTo>
  <wsa:To>xs:anyURI</wsa:To>
   <osci:TypeOfBusinessScenario @wsa:IsReferenceParameter="1">
    xs:anyURI
   </osci:TypeOfBusinessScenario>
  ...
 </s12:Header>
 <s12:Body ...>
  <osci:MsgBoxFetchRequest>
   <osci:EPR> wsa:EndpointReference </osci:EPR>
    <osci:MsgSelector newEntry=("true" | "false")>
     <osci:MessageId> xs:anyURI </osci:MessageId> *
     <osci:RelatesTo> xs:anyURI </osci:RelatesTo> *
     <osci:MsgBoxEntryTimeFrom>
         xs:dateTime
     </osci:MsgBoxEntryTimeFrom> ?
     <osci:MsgBoxEntryTimeTo> xs:dateTime </osci:MsgBoxEntryTimeTo> ?
     <osci:Extension> xs:anyType </osci:Extension> ?
    </osci:MsgSelector> ?
  </osci:MsgBoxFetchRequest>
 </s12:Body>
</s12:Envelope>
```

The following describes normative constraints on the outline listed above:

`/s12:Envelope/s12:Header/wsa:Action`

The value indicated herein MUST be used for that URI.

`/s12:Envelope/s12:Header/wsa:MessageID`

The request MUST carry a unique WS-Addressing MessageID.

/s12:Envelope/s12:Header/wsa:ReplyTo

The Endpoint Reference (EPR) of the requesting Recipient endpoint. As MsgBoxFetchRequests are considered to only being meaningful in synchronous request-response MEPs, the EPRs address element MUST be restricted to the anonymous URI.

/s12:Envelope/s12:Header/wsa:To

The address of the MsgBox (request destination) endpoint.

/s12:Envelope/s12:Header/osci:TypeOfBusinessScenario

This value of the instantiation of **/wsa:ReferenceParameters** MUST be supplied for this message type. The value of **/osci:TypeOfBusinessScenario** is taken as message selection argument and SHOULD match one of those accepted by this endpoint.

/s12:Envelope/s12:Header/osci:TypeOfBusinessScenario/
@wsa:IsReferenceParameter

Following WS-Addressing, the element MUST be attributed with **@wsa:IsReferenceParameter="1"**

The body of this message contains the actual request in a structure

/s12:Envelope/s12:Body/osci:MsgBoxFetchRequest.

/s12:Envelope/s12:Body/osci:MsgBoxFetchRequest/osci:EPR

The Endpoint Reference (EPR) of the message box endpoint where the requested messages are to be pulled from; type is wsa:EndpointReferenceType. This is the only element which MUST be present in a MsgBoxFetchRequest. Only messages originally targeted to this EPR MUST be returned. The EPR MUST contain reference properties to help uniquely identify the source endpoint according to chapter [6, Addressing Endpoints].

If a MsgBoxFetchRequest contains no other arguments for message selection, the messages to be selected MUST be those which have not yet been fetched. Those are all messages in the addressed MsgBox which have no SOAP header element or a value of zero in the time instant element .../**osci:MsgTimeStamps/osci:InitalFetched.** They MUST be delivered one per request-/ response in a FIFO-manner to the endpoint denoted by **/s12:Envelope/s12:Header/wsa:ReplyTo**.

/s12:Envelope/s12:Body/osci:MsgBoxFetchRequest/osci:MsgSelector ?

If this optional element is present, arguments of the attribute **@newEntry** and sub-elements MsgSelector MUST be processed as logical AND (after first OR-Processing of the sequences of MessageIDs in the SOAP body elements **.../osci:MessagID** and **.../osci:RelatesTo**, if present).

/s12:Envelope/s12:Body/osci:MsgBoxFetchRequest/osci:MsgSelector/@newEntry ?

This optional boolean attribute is defaulted to a value of true, if not present. If present, this attribute denotes whether only already pulled or new entered messages have to be selected from the MsgBox. "New" messages are indicated by having no SOAP header element or a value of zero in the time instant element .../**osci:MsgTimeStamps/osci:InitalFetched.**

/s12:Envelope/s12:Body/osci:MsgBoxFetchRequest/osci:MsgSelector/
osci:MessageID *

If present, this element contains a sequence of WS-Addressing MessageIDs. By including this element the request a MsgBox service MUST limit its search to just those messages with these values in the WS-Addressing SOAP header element **.../wsa:MessageID.**

/s12:Envelope/s12:Body/osci:MsgBoxFetchRequest/osci:MsgSelector/
osci:RelatesTo *

If present, this element contains a sequence of WS-Addressing MessageIDs. By including this element the request a MsgBox service MUST limit its search to just those messages with these values in the WS-Addressing SOAP header elements **.../wsa:RelatesTo.**

/s12:Envelope/s12:Body/osci:MsgBoxFetchRequest/osci:MsgSelector/
osci:MsgBoxEntryTimeFrom ?

If present, this element denotes a value of type **xs:dateTime** as lower value when a message has been accepted by a MsgBox service. The resulting search expression is …**/osci:MsgBoxEntryTimeFrom** >= the value of …**/osci:Delivery** in the message SOAP header block **osci:MsgTimeStamps** if the correlated element …/**osci:MsgBoxEntryTimeTo** is not present in …**/osci:MsgSelector**.

/s12:Envelope/s12:Body/osci:MsgBoxFetchRequest/osci:MsgSelector/
osci:MsgBoxEntryTo ?

If present, this element denotes a value of **xs:dateTime** as upper value when a message has been accepted by a MsgBox services. The resulting search expression is …**/osci:MsgBoxEntryTimeTo** <= the value of …**/osci:Delivery** in the message SOAP header block **osci:MsgTimeStamps** if the correlated element …/**MsgBoxEntryTimeFrom** is not present in …**/osci:MsgSelector**.

If latter elements both are set, the resulting search expression is …**/osci:MsgBoxEntryFrom** >= **.../osci:Delivery** <= …**/osci:MsgBoxEntryTimeTo**; the value of …**/osci:MsgBoxEntryFrom** MUST be less or equal to the value of …**/osci:MsgBoxEntryTo**.

/s12:Envelope/s12:Body/osci:MsgBoxFetchRequest/osci:MsgSelector/
osci:Extension/{any} *

This is an extensibility mechanism to allow other search criteria to be passed. For example, an XPath query could be used to search for messages that match a certain pattern. Implementations may use this element for defining search criteria on agreements outbound to this specification. At some future time this specification will define such an extension.

Upon receipt and authentication of this message, the MsgBox service MUST locate any message that matches the selection criteria. Only messages originally targeted to this EPR MUST be returned. The search criteria MUST include examination of the child elements inside the SOAP body element …**/osci:MsgSelector**.

Selected messages MUST be given back to the requestor one by one in the response to this request in an ascending order given by the values of the SOAP header block element **/osci:MsgTimeStamps/osci:Delivery** ("FIFO"). A MsgBox service MUST hold the complete list corresponding to the selection criteria and deliver an ID for this list to the requestor with the response. In subsequent requests (see MsgBoxGetNextRequest in chapter [8.2.4]) the Requestor is able to pull further messages of a selection result with reference to this list. Remaining messages of the complete list MUST be retained for following messages of type MsgBoxGetNextRequest.

8.2.2 MsgBoxStatusListRequest

To request a message status list from a MsgBox service endpoint, a requestor MUST send a MsgBoxStatusListRequest message to his MsgBox instance endpoint.

The normative outline for a MsgBoxStatusListRequest request is akin to the MsgBoxFetchRequest:

```
<s12:Envelope ...>
 <s12:Header ...>
  ...
```

```
  <wsa:Action>
http://www.osci.eu/ws/2008/05/transport/urn/messageTypes/MsgBoxStatusListRe
quest
  </wsa:Action>
  <wsa:MessageID>xs:anyURI</wsa:MessageID>
  <wsa:ReplyTo> wsa:EndpointReference </wsa:ReplyTo>
  <wsa:To>xs:anyURI</wsa:To>
   <osci:TypeOfBusinessScenario @wsa:IsReferenceParameter="1">
    xs:anyURI
   </osci:TypeOfBusinessScenario>

  ...
 </s12:Header>
 <s12:Body ...>
     <osci:MsgBoxStatusListRequest maxListItems="xs:positiveInteger>
   <osci:EPR> wsa:EndpointReference </osci:EPR>
    <osci:MsgSelector newEntry=("true" | "false")>
     <osci:MessageId> xs:anyURI </osci:MessageId> *
     <osci:RelatesTo> xs:anyURI </osci:RelatesTo> *
     <osci:MsgBoxEntryTimeFrom>
       xs:dateTime
     </osci:MsgBoxEntryTimeFrom> ?
     <osci:MsgBoxEntryTimeTo>
       xs:dateTime
     </osci:MsgBoxEntryTimeTo> ?
     <osci:Extension> xs:anyType </osci:Extension> ?
    </osci:MsgSelector> ?
  </osci:MsgBoxStatusListRequest>
 </s12:Body>
</s12:Envelope>
```

Description of normative constraints on the outline listed above:

`/s12:Envelope/s12:Header/wsa:Action`

The value indicated herein MUST be used for that URI.

`/s12:Envelope/s12:Header/wsa:MessageID`

The request MUST carry a unique WS-Addressing MessageID.

`/s12:Envelope/s12:Header/wsa:ReplyTo`

The Endpoint Reference (EPR) of the requesting Recipient endpoint. As message box requests considered to only being meaningful in synchronous request-response message MEPs, the EPRs address element MUST be restricted to the anonymous URI.

`/s12:Envelope/s12:Header/wsa:To`

The address of the MsgBox (request destination) endpoint.

`/s12:Envelope/s12:Header/osci:TypeOfBusinessScenario`

This value of the instantiation of **`/wsa:ReferenceParameters`** MUST be supplied for this message type. The value of **`/osci:TypeOfBusinessScenario`** is taken as message selection argument and SHOULD match one of those accepted by this endpoint. To select the message status list for all messages in this MsgBox instance, a value of "*" MAY be supplied here.

`/s12:Envelope/s12:Header/osci:TypeOfBusinessScenario/`
`@wsa:IsReferenceParameter`

Following WS-Addressing, the element MUST be attributed with **`@wsa:IsReferenceParameter="1"`**

The body of this message contains the actual request in the structure

`/s12:Envelope/s12:Body/osci:MsgBoxStatusListRequest.`

/s12:Envelope/s12:Body/osci:MsgBoxStatusListRequest/@maxListItems ?

The requestor MAY limit the length of the message status list he expects in the response with this attribute of type **xs:positiveInteger**. A MsgBox service MUST hold the complete list corresponding to the selection criteria and deliver an ID for this list to the requestor with the response. In subsequent requests (see MsgBoxGetNextRequest in chapter [8.2.4]), the requestor is able to request further portions of a selection result with reference to this list.

A MsgBox instance MAY limit the value of **@maxListItems** to any value greater zero.

If provided, a MsgBox instance MUST retain this value – if not decreased by its configured limit - together with the result set until the whole result set is delivered to the requestor or the requestor cancels an iteration sequence (see MsgBoxCloseRequest in chapter [8.2.5].

/s12:Envelope/s12:Body/osci:MsgBoxStatusListRequest/osci:EPR

The EPR of the message box endpoint where the requested message status list has to be pulled from; type is **wsa:EndpointReferenceType**. This is the only element which MUST be present in a MsgBoxFetchRequest. Only status lists of messages originally targeted to this EPR MUST be returned. The EPR MUST contain **wsa:ReferenceParameters** to help uniquely identify the source endpoint according to chapter [6, Addressing Endpoints]. If a MsgBoxFetchRequest contains no other arguments for message selection, the messages to be selected MUST be those which have not yet been fetched. That are all messages in the addressed MsgBox having no SOAP header element or a value of zero in the **…/osci:MsgTimeStamps/osci:InitalFetched** time instant element.

While for a …**/osci:MsgBoxFetchRequest** the EPR has to be specified completely including the type of business scenario in …**/wsa:ReferenceParameters** according to chapter [6, Addressing Endpoints], for the MsgBoxStatusListRequest it is possible to supply the element …**/wsa:ReferenceParameters/osci:TypeOfBusinessScenario** with a value of **"*"**. This entry MUST lead to a message box status list containing all messages with no regard to a specific addressed business scenario of this endpoint actually exposes to be able to serve.

/s12:Envelope/s12:Body/osci:MsgBoxStatusListRequest/osci:MsgSelector

For the content of this complex element, which defines selection criteria for messages, see description in last chapter [8.2.1].

/s12:Envelope/s12:Body/osci:MsgBoxStatusListRequest/osci:MsgSelector/ osci:Extension/{any} *

This is an extensibility mechanism to allow other search criteria to be passed. See respective explanation for **osci:MsgBoxStatusListRequest.**

Upon receipt and authentication of this message, the MsgBox service will locate any message that matches the selection criteria. Only messages originally targeted to this EPR MUST be selected for the required message status list. The search criteria MUST include examination of the child elements inside the **/osci:MsgSelector** SOAP body element.

The message status list to be given back to the requestor MUST be of the maximum size denoted by **/osci:MsgBoxStatusListRequest/@maxListItems** or a lower size according to possible configured restrictions of the requested MsgBox instance. The list MUST be build up and sorted in an ascending order given by the message SOAP header block element **/osci:MsgTimeStamps/osci:Delivery** ("FIFO"). Remaining items of the complete list not deliverable to the requestor directly in the response to the initial MsgBoxStatusListRequest MUST be retained for following messages of type MsgBoxGetNextRequest.

8.2.3 MsgBoxResponse

Request messages MsgBoxFetchRequest und MsgBoxStatusListRequest are both responded by the same status information in the SOAP header block of the response, only the body parts differ as outlined in the following chapters.

The normative outline for a MsgBoxResponse header is:

```
<s12:Envelope ...>
 <s12:Header ...>
  ...
   <wsa:Action>
    http://www.osci.eu/ws/2008/05/transport/urn/messageTypes/MsgBoxResponse
   </wsa:Action>
   <wsa:MessageID>xs:anyURI</wsa:MessageID>
   <wsa:FaultTo> wsa:EndpointReference </wsa:FaultTo> ?
   <wsa:To>xs:anyURI</wsa:To>
   ...
  <osci:MsgBoxResponse MsgBoxRequestID="xs:anyURI"
     wsu:Id = "xs:ID" ?
       <osci:NoMessageAvailable reason=xs:QName/>
       |
       <osci:ItemsPending resultIteratorID=xs:positiveInteger ?
          xs:positveInteger
       </osci:ItemPending>
   </osci:MsgBoxResponse>
  ...
 </s12:Header>
 <s12:Body ...>

 </s12:Body>
</s12:Envelope>
```

Description of normative constraints on the outline listed above (WS-Addressing header elements are to be handled according to chapter [6, Addressing Endpoints]):

`/s12:Envelope/s12:Header/wsa:Action`

The value indicated herein MUST be used for that URI.

`/s12:Envelope/s12:Header/wsa:MessageID`

The request MUST carry a unique WS-Addressing MessageID.

`/s12:Envelope/s12:Header/wsa:FaultTo ?`

The optional Endpoint Reference (EPR) SOAP fault messages should be routed to.

`/s12:Envelope/s12:Header/wsa:To`

The address of the endpoint of the initial requestor, derived from the **`/wsa:ReplyTo`** header element of the corresponding MsgBox request.

`/s12:Envelope/s12:Header/osci:MsgBoxResponse`

The container for the status response; the status response is a choice of two alternatives, depending on request fulfilment.

Following attributes MUST be set:

`/s12:Envelope/s12:Header/osci:MsgBoxResponse/@MsgBoxRequestID`

This mandatory element of type **`xs:anyURI`** MUST carry a unique value of type UUID according to [RFC4122]. It serves to identify messages of type MsgBoxFetchRequest and MsgBoxStatusListRequest and MUST be used by the Requestor in subsequent messages of type MsgBoxGetNextRequest or MsgBoxCloseRequest explained below. The value MUST be generated by a MsgBox instance for every incoming MsgBoxFestRequest or

MsgBoxStatusListRequest and MUST be retained and correlated to these requests with their individual search criteria.

/s12:Envelope/s12:Header/osci:MsgBoxResponse/@wsu:Id ?

For ease of referencing this SOAP body block, this optional attribute of type **wsu:Id** MAY be provided.

/s12:Envelope/s12:Hedader/osci:MsgBoxResponse/osci:NoMessageAvailable

This element of the choice of **. . . /MsgBoxResponse** MUST be set if

- there are no messages available corresponding to the selection criteria
- there where errors detected in the selection criteria.

The element carries following attribute:

/s12:Envelope/s12:Header/osci:MsgBoxResponse/osci:NoMessageAvailable/ @reason ?

Attribute of type **xs:QName**, identifies the reason of **/osci:NoMessageAvailable** set.

The alternate of the choice of .../**MsgBoxResponse** MUST be set if there are – according to the selection criteria of the request - messages or message status list items pending (not yet deliverable to the requestor in the actual response):

/s12:Envelope/s12:Header/osci:MsgBoxResponse/osci:ItemsPending

This element of type **xs:nonNegativeInteger** MUST be set with the number of the remaining items. If the last portion of a result set delivered to the requestor with this actual response, the value MUST be set to zero to signal this fact.

8.2.3.1 MsgBoxResponse - body to MsgBoxFetchRequest

For this type of foregoing initial request, the requested message MUST be delivered in following manner:

- A SOAP Envelope with all child elements MUST be build up containing a header block with the ones of the original message except header elements which had initially been targeted to and successfully executed by the MsgBox node as well as the transport encryption and signature elements which had been supplied by the Initiator of this message.
- The SOAP header element **osci:MsgTimeStamps** MUST be inserted (or completed, if present) as described in chapter [8.1].
- All original WS-Addressing, **osci:X509TokenContainer** , **xkms:ValidateResult** (inside a **xkms:CompoundResult**) and original Security Token and WS-Trust header elements MUST be included.
- If present in the original message, the **osci:ReceptionReceiptDemand** header element MUST be included.
- The original SOAP body child elements MUST be included unchanged as child elements of the SOAP body of this SOAP Envelope to be build up.
- The Recipient may have interest in the authentication and authorization data originally carried in the SOAP WS Security header when delivering a message to the Recipients MsgBox. Therefore, this security token MUST be inserted as additional child element in the SOAP header of this SOAP Envelope to be built up.

The resulting SOAP envelope MUST be included as child element of the SOAP body block of the response message.

8.2.3.2 MsgBoxResponse - body to MsgBoxStatusListRequest

For this type of foregoing initial request, the requested list MUST be build up in the SOAP body block of the response message. This is the same for responses to subsequent requests of type MsgBoxGetNextRequest (see MsgBoxGetNextRequest in chapter [8.2.4]).

The normative outline for a MsgStatusList is:

```
<osci:MsgStatusList>
  <osci:MsgAttibutes>
    <wsa:MessageID>xs:anyUri</wsa:MessageID>
    <wsa:RelatesTo>xs:anyUri</wsa:RelatesTo> *
    <wsa:From>endpoint-reference</wsa:From>
    <osci:TypeOfBusinessScenario>xs:anyUri</osci:TypeOfBusinessScenario>
    <wsa:Action>xs:anyUri</wsa:Action>
    <osci:MsgSize>xs:positiveInteger</osci:msgSize>
    <osci:ObsoleteAfterDate> xs:date </osci:ObsoleteAfterDate> ?
    <osci:DeliveryTime> xs:dateTime </osci:DeliveryTime>
    <osci:InitialFetchTime> xs:dateTime </osci:InitialFetchTime> ?
  </osci:MsgAttributes> *
</osci:MsgStatusList>
```

The whole structure MUST be positioned under **`/s12:Envelope/s12:Body.`**

`/osci:MsgStatusList`

Container for the items of the list.

`/osci:MsgStatusList/osci:MsgAttributes *`

The container for the attributes of one message of the status list. The number of occurrences is determined by the number of items of selection result list not yet delivered to the requestor and the value of …**`/osci:MsgBoxStatusListRequest/@maxListItems`** of the initial MsgBoxStatusListRequest, which MAY be modified to a lower value greater zero set by the requested MsgBox instance.

`/osci:MsgStatusList/osci:MsgAttributes/wsa:MessageID`

MessageID of the message, derived from respective header element.

`/osci:MsgStatusList/osci:MsgAttributes/wsa:RelatesTo *`

MessageIDs of related messages of the message, derived from respective header elements.

`/osci:MsgStatusList/osci:MsgAttributes/wsa:From`

From-EPR of the message, derived from the respective header element.

`/osci:MsgStatusList/osci:TypeOfBusinessScenario`

This URI denotes the type of addressed business scenario of the intended recipient of the message. It is derived from the **`/wsa:ReferenceParameters /osci:TypeOfBusinessScenario`** associated to the WS-Addressing SOAP header element **`/wsa:To`** of the message.

`/osci:MsgStatusList/wsa:Action`

Derived from respective SOAP header element /**`wsa:Action`** set in the message.

`/osci:MsgStatusList/osci:MsgSize`

The size of the message in kilobytes has to be supplied here as **`xs:positiveInteger`**.

Following timestamps are provided in an **`osci:MsgStatusList`** according to the **`/osci:MsgTimeStamps`** described in chapter [8.1]:

`/osci:MsgStatusList/ObsoleteAfterDate ?`

Optional element of type **xs:date**, contains - if present in the underlying message - the value of the SOAP header block element **/osci:MsgTimeStamps/osci:ObsoleteAfter** present in the underlying message.

/osci:MsgStatusList/DeliveryTime

This element of type **xs:dateTime** contains the value of the SOAP header block element …**/osci:MsgTimeStamps/osci:Delivery**, which MUST be present in a message stored by a MsgBox instance.

/osci:MsgStatusList/InitialFetchedTime ?

This optional element of type **xs:dateTime** contains the value of the SOAP header block element …**/osci:MsgTimeStamps/osci:InitialFetched,** which MAY be present in a message stored by a MsgBox instance. Only if not present or present with a value of zero, the MsgBox instance MUST provide this element with his actual server time before message delivery.

8.2.4 MsgBoxGetNextRequest

To request subsequent, not yet delivered results from foregoing requests of type MsgBoxStatusListRequest or MsgBoxFetchRequest, a requestor MUST send a MsgBoxGetNextRequest message to the same MsgBox instance.

The normative outline for a MsgBoxGetNextRequest:

```
<s12:Envelope ...>
 <s12:Header ...>
  ...
   <wsa:Action>
   http://www.osci.eu/ws/2008/05/transport/urn/messageTypes/
        MsgBoxGetNextRequest
   </wsa:Action>
   <wsa:MessageID>xs:anyURI</wsa:MessageID>
   <wsa:ReplyTo>endpoint-reference</wsa:ReplyTo>
   <wsa:To>xs:anyURI</wsa:To>
    <osci:TypeOfBusinessScenario @wsa:IsReferenceParameter="1">
     xs:anyURI
    </osci:TypeOfBusinessScenario>

   ...
 </s12:Header>
 <s12:Body ...>
  <osci:MsgBoxGetNextRequest MsgBoxRequestID="xs:anyURI">
   <osci:EPR>MsgBox EPR</osci:EPR>
 <osci:LastMsgReceived> wsa:MessageID </osci:LastMsgReceived> *
  </osci:MsgBoxGetNextRequest>
 </s12:Body>
</s12:Envelope>
```

Description of normative constraints on the outline listed above:

/s12:Envelope/s12:Header/wsa:Action

The value indicated herein MUST be used for that URI.

/s12:Envelope/s12:Header/wsa:MessageID

The request MUST carry a unique WS-Addressing MessageID.

/s12:Envelope/s12:Header/wsa:ReplyTo

The EPR of the requesting (source-) endpoint. As message box requests considered to only being meaningful in synchronous request-response scenarios, EPRs address element MUST be restricted to the anonymous URI.

/s12:Envelope/s12:Header/wsa:To

The address of the MsgBox (request destination) endpoint.

/s12:Envelope/s12:Header/osci:TypeOfBusinessScenario

The corresponding value of the initial MsgBoxFetchRequest or MsgBoxStatusListRequest MUST be supplied for this message type.

/s12:Envelope/s12:Header/osci:TypeOfBusinessScenario/ @wsa:IsReferenceParameter

Following WS-Addressing, the element MUST be attributed with **@wsa:IsReferenceParameter="1"**

The body of this message contains the actual **/s12:Envelope/s12:Body/osci:MsgBoxGetNextRequest.**

/s12:Envelope/s12:Body/osci:MsgBoxGetNextRequest/@MsgBoxRequestID

This attribute of type **xs:anyURI** MUST be provided with the value of the with this message referenced foregoing **MsgBoxResponse/@MsgBoxRequestID.** The MsgBox service MUST use it to correlate this MsgBoxGetNextRequest to the initial MsgBoxFetchRequest respective MsgBoxStatusListRequest.

/s12:Envelope/s12:Body/osci:MsgBoxGetNextRequest/osci:EPR

The EPR of the message box endpoint where the next requested message status list respective message has to be pulled from, type is **wsa:EndpointReferenceType**. This element SHOULD be interpreted from the MsgBox service for verifying the same EPR is still requested as it has been in the initial request – if consistence of such request sequences is not secured by other mechanisms.

/s12:Envelope/s12:Body/osci:MsgBoxGetNextRequest/osci:LastMsgReceived *

These optional elements of type **wsa:AttributedURIType** MAY be provided, when the underlying initial request was of the type MsgBoxFetchRequest. The requestor SHOULD provide here the value(s) of the **/wsa:MessageID** of the last message(s) he received in the body of the foregoing response(s) to commit successful reception of those messages. This has to be realized as "reception acknowledge by requester" by the MsgBox instance: If the SOAP header element .../**osci:MsgTimeStamps/osci:Reception** is absent or the value of the SOAP header element **.../osci:MsgTimeStamps/osci:Reception** is zero, the actual server time of the MsgBox instance MUST now be set here and the value has to be be signed according to chapter [8.1]. The resulting changes in the SOAP header block **/osci:MsgTimeStamps** now MUST be persisted in the MsgBox store.

Upon receipt and authentication of this message, the MsgBox service MUST – depending on type of initial request referenced by **osci:MsgBoxGetNextRequest/@MsBoxRequestID**

– deliver a MsgBoxResponse with the next message of the list indicated by **/osci:MsgBoxResponse/@MsBoxRequestID** in the body of the response (rules denoted in chapter [8.2.3.1] apply)

– deliver a MsgBoxResponse with the next portion of a **/osci:MsgStatusList** indicated by **/osci:MsgBoxResponse/@MsBoxRequestID** in the body of the response (rules denoted in chapter [8.2.3.2] apply).

Inside the SOAP header element …**/osci:MsgBoxResponse**, choice …**/osci:ItemsPending** MUST be set to the actual value. If …**/osci:ItemsPending** becomes a value auf zero now, this fact signal the requestor that the MsgBox instance may have discarded the search result list referenced by the identifier **/osci:MsgBoxResponse/@MsBoxRequestID**.

8.2.5 MsgBoxCloseRequest

The functionalities of this message type are:

- Recipient commits successful reception of messages from his MsgBox instance

- Recipient signals the abortion of an iterative pull process of sequences of result requests of foregoing initial MsgBoxFetchRequest respective MsgBoxStatusListRequest.

NOTE: In case of sussecful processing of a MsgBoxCloseRequest by the targeted MsgBox instance a response MUST NOT be generated.

The normative outline for the MsgBoxCloseRequest:

```
<s12:Envelope ...>
 <s12:Header ...>
  ...
  <wsa:Action>
http://www.osci.eu/ws/2008/05/transport/urn/messageTypes/MsgBoxCloseRequest
  </wsa:Action>
  <wsa:MessageID>xs:anyURI</wsa:MessageID>
  <wsa:ReplyTo>endpoint-reference</wsa:ReplyTo>
  <wsa:To>xs:anyURI</wsa:To>
   <osci:TypeOfBusinessScenario @wsa:IsReferenceParameter="1">
    xs:anyURI
   </osci:TypeOfBusinessScenario>

  ...
 </s12:Header>
 <s12:Body ...>
  <osci:MsgBoxCloseRequest MsgBoxRequestID="xs:anyURI">
   <osci:LastMsgReceived>xs:anyURI</LastMsgReceived> *
  </osci:MsgBoxCloseRequest>
 </s12:Body>
</s12:Envelope>
```

Description of normative constraints on the outline listed above:

`/s12:Envelope/s12:Header/wsa:Action`

The value indicated herein MUST be used for that URI.

`/s12:Envelope/s12:Header/wsa:MessageID`

The request MUST carry a unique WS-Addressing MessageID.

`/s12:Envelope/s12:Header/wsa:ReplyTo`

The EPR of the requesting (source-) endpoint. As message box requests considered to only being meaningful in synchronous request-response scenarios, EPRs Address element MUST be restricted to the anonymous URI.

`/s12:Envelope/s12:Header/wsa:To`

The address of the MsgBox (request destination) endpoint.

`/s12:Envelope/s12:Header/osci:TypeOfBusinessScenario`

The corresponding value of the initial MsgBoxFetchRequest or MsgBoxStatusListRequest MUST be supplied for this message type.

`/s12:Envelope/s12:Header/osci:TypeOfBusinessScenario/`
`@wsa:IsReferenceParameter`

Following WS-Addressing, the element MUST be attributed with **`@wsa:IsReferenceParameter="1"`**

The body of this message contains the actual **`/s12:Envelope/s12:Body/osci:MsgBoxCloseRequest.`**

`/s12:Envelope/s12:Body/osci:MsgBoxGetNextRequest/@MsgBoxRequestID`

This attribute of type **`xs:anyURI`** MUST be provided with the value of the with this message referenced foregoing **`MsgBoxResponse/@MsgBoxRequestID.`** The MsgBox

service MUST use it to correlate this MsgBoxCloseRequest to the initial MsgBoxFetchRequest respective MsgBoxStatusListRequest.

/s12:Envelope/s12:Body/osci:MsgBoxCloseRequest/LastMsgReceived ?

These optional elements of type **wsa:AttributedURIType** MAY be provided, when the underlying initial request was of the type MsgBoxFetchRequest. The requestor SHOULD provide here the value(s) of the **/wsa:MessageID** of the last message(s) he received in the body of the foregoing response(s) to commit successful reception of those messages. This has to be realized as "reception acknowledge by requester" by the MsgBox instance: If the SOAP header element …**/osci:MsgTimeStamps/osci:InitialFetched** is absent or present with a value of zero, the actual server time of the MsgBox instance MUST now be set here and the value has to be signed according to chapter [8.1]. The resulting changes in the SOAP header block **/osci:MsgTimeStamps** now MUST be persisted in the MsgBox store.

It should be noted, that this message type MUST be send to the MsgBox instance ever when a MsgBoxFetchRequest was the initial message send and the requestor pulled a message successfully the first time (a new message). This triggers the commitment of the SOAP header **/osci:MsgTimeStamps/osci:Reception** and **/osci:MsgTimeStamps/osci:InitialFetched** time instances. *It is up to implementations of recipient instances, how distinct between "new" and already processed messages*, because the recipient transport gateway has no implicit control on the state of the successful body processing (for example to mark message as "readed" or "processed" – this at least is under the control of the application targeted by the message).

To avoid situations, where successful pulled messages on the MsgBox instance side remain in the state unpulled, it is strongly recommended to commit every MsgBoxResponse to an initial MsgBoxFetchRequest and following series of MsgBoxGetNextRequest.

8.2.6 Processing Rules for MsgBoxGetNext/CloseRequest

MsgBox instances are free to to configure a timeout value to retain search result list identified by **/osci:MsgBoxResponse/@MsgBoxRequestID.**

If a MsgBox instance receives a MsgBoxGetNextRequest or a MsgBoxCloseRequest not at all or not more known here, no processing on the message database must be done and a following fault MUST be generated:

Fault 7: **MsgBoxRequestWrongReference**	
[Code]	Sender
[Subcode]	MsgBoxRequestWrongReference
[Reason]	MsgBoxRequestID unknown or timed out.

8.3 Receipts

Requirements for receipting message exchange were outlined in "OSCI-Transport 2.0 – Functional Requirements and Design Objectives“ and "OSCI-Transport 2 – Technical Features Overview"

Besides provableness of what has been delivered / received when, for messages exchange patterns using the MsgBox service it may be of interest for the Initiator to be informed, when the intended Recipient pulls the message from his MsgBox. More concrete – the business scenario needs of an asynchronous message are bound to reaction times. In this case, a service requestor has to have control to in-time delivery to the targeted Recipient. In doubt there isn't any Recipient activity concerning the request, a service requestor (or even responder) may choose other communication channels to get in contact.

As there may be non-conformant implementations which don't answer to a requested ReceptionReceipt, for additional comfort of control whether a message has been pulled yet by the intended Recipient, the construct of a **FetchedNotification** is foreseen, which alike described for receipts can be demanded by Initiator and Recipient instances. If requested, the Recipients MsgBox instance MUST deliver such a notification to the endpoint the Initiator specified in his message; contents are the SOAP header elements indicating source and destination of the message and the time instant when it is pulled by the intended Recipient. No separate signature is foreseen for this notification. The FetchedNotification is delivered in the SOAP body of a separate osci:Request to the endpoint to be exposed in the demand for this FetchedNotification – which again in general should be the MsgBox of the requesting Initiator or Recipient node.

8.3.1 Demanding Receipts

To demand receipts and define its details, for each specific demand the here defined SOAP header blocks MAY be provided in outbound messages of type osci:Request and osci:Response by SOAP/OSCI endpoints (Initiator or Recipient).

8.3.1.1 Demand for Delivery Receipt

If the next logical OSCI node a message of type osci:Request is targeted to shall deliver a DeliveryReceipt in the backchannel osci:Response message, following SOAP header block MUST be included in the message:

```
<osci:DeliveryReceiptDemand @wsu:Id="xs:ID"
   @s12:role=
      "http://www.w3.org/2003/05/soap-envelope/role/next" ?
   @s12:mustUnderstand= "true" | "false" ?
   @qualTSPforReceipt="true" | "false" ?
   @echoRequest= "true" | "false") ? >
  <wsa:ReplyTo> wsa:EndpointReference <wsa:ReplyTo>
</osci:DeliveryReceiptDemand> ?
```

Description of elements and attributes in the schema overview above:

`/osci:DeliveryReceiptDemand ?`

Optional SOAP header for indicating requirements for a DeliveryReceipt. It MUST be provided under the conditions mentioned above.

`/osci:DeliveryReceiptDemand/@wsu:Id`

This attribute of type **`wsu:Id`** SHOULD be provided so that un-ambiguous references can be made to this element.

`/osci:DeliveryReceiptDemand/@s12:role`

This attribute of type **`xs:anyURI`** MAY be provided. It defaults to the URI outlined above. If this attribute is provided, it MUST be set to this value. Following the semantics of

[SOAP12], this SOAP header block is designated to next SOAP-node passed on the message route.

/osci:DeliveryReceiptDemand/@s12:mustUnderstand

This boolean attribute SHOULD be provided with a value of "true". Following the semantics of [SOAP12], this SOAP header block MUST be understood and processed by the next SOAP-node passed on the message route willing to act in the role denoted by the foregoing attribute **/osci:ReceiptDemand/@s12:role.** For interoperability reasons with Web Service implementations not able to process the receipts defined here, it may be set to "false" or not present (which is equivalent to a value of "false").

/osci:DeliveryReceiptDemand/@qualTSPforReceipt ?

This optional boolean attribute signals – if set to a value of "true" – a qualified timestamp for the receipt information is requested. If such a service is not available on the node the receipt is demanded from, a fault (see chapter [8.3.2]) MUST be generated to the requesting node and the incoming message MUST be discarded.

/osci:DeliveryReceiptDemand/@echoRequest ?

This optional boolean attribute signals – if set to a value of "true" – the requesting node requires the retransmission of the whole message in the required receipt. In this case, the node the receipt is demanded from MUST provide the whole message in binary format in the receipt part of the response message (see chapter [8.3.2.1]). Care should be taken to use this feature with regard to caused overhead and bandwidth consumption.

If absent, this attribute defaults to a value of "false".

/osci:DeliveryReceiptDemand/wsa:ReplyTo

This required element of type **wsa:EndpointReferenceType** denotes the endpoint, where the requestor wishes the receipt should be routed to. In case of a DeliveryReceipt demand in a message of type osci:Request, the value herein for .../**wsa:Address** SHOULD be **http://www.w3.org/2005/08/addressing/anonymous;** the DeliveryReceipt is returned directly in the header of the response to the incoming message in the same http-connection.

In case the requestor wishes a DeliveryReceipt should be routed some specialized endpoint consuming receipts the EPR of the endpoint MUST be exposed here. The DeliveryReceipt is this case MUST be delivered in the SOAP body of a separate new osci:Request message. Hence, this EPR SHOULD be the one of the MsgBox instance of the requestor. It MAY even be a specialized endpoint consuming receipts. The EPR MUST contain reference properties according to chapter [6, Addressing Endpoints]. A …**/wsa:ReferenceParameters** of following value SHOULD be provided:

<osci:TypeOfBusinessScenario>
www.osci.eu/2008/common/urn/messageTypes/Receipt
</osci:TypeOfBusinessScenario>.

In case of delivering a receipt to a MsgBox instance, this is the defaulted value for separating receipt message types from other ones (see chapter [6, Addressing Endpoints]).

A **/osci:DeliveryReceiptDemand** header block MUST NOT be included in an osci:Response message. As for an osci:Response, there is no network backchannel available; in this case DeliveryReceipt could not be delivered in the standard manner. If provability of response delivery is needed, an **/osci:ReceptionReceiptDemand** should be used instead.

For synchronous request-response scenarios driven point-to-point between instances of initiator and recipient, it is advisable to economize demands for receipts to avoid overhead and processing of not needed DeliveryReceipts. Provability of communication here MAY be gained by a reception receipt

requirement positioned in one or more messages of the request-response sequence, depending on underlying concrete business process needs. Certainty of delivery itself is implicit given by successful processing of such a scenario.

8.3.1.2 Demand for ReceptionReceipt

If an endpoint a message if type osci:Request or osci:Response is targeted to shall deliver a ReceptionReceipt, following SOAP header block MUST be included in the message. The underlying schema is the same as for an **`osci:DeliveryReceiptDemand`** SOAP header block; possible attribute/element values and semantics differ in detail as described below.

```
<osci:ReceptionReceiptDemand @wsu:Id="..."
   @s12:role=
      "http://www.w3.org/2003/05/soap-envelope/role/ultimateReceiver" ?
   @s12:mustUnderstand= "true" | "false" ?
   @qualTSPforReceipt="true" | "false" ?
   @echoRequest= "true" | "false") ? >
  <wsa:ReplyTo> wsa:EndpointReference <wsa:ReplyTo>
</osci:ReceptionReceiptDemand> ?
```

Description of elements and attributes in the schema overview above:

`/osci:ReceptionReceiptDemand ?`

Optional SOAP header for indicating requirements for a ReceptionReceipt.

`/osci:ReceptionReceiptDemand/@wsu:Id`

This attribute of type **`wsu:Id`** SHOULD be provided so that un-ambiguous references can be made to this element.

`/osci:ReceptionReceiptDemand/@s12:role`

This attribute of type **`xs:anyURI`** MAY be provided. It defaults to the URI outlined above. If this attribute is provided, it MUST be set to this value; following the semantics of [SOAP12], this SOAP header block is designated SOAP-node acting in the role of a ultimate receiver – which is the node at least the SOAP body is designated to, corresponding to the UltimateRecipient node in the role model of this specification.

`/osci:ReceptionReceiptDemand/@s12:mustUnderstand`

This boolean attribute SHOULD be provided with a value of "true". Following the semantics of [SOAP12], this SOAP header block MUST be understood and processed by the next SOAP-node passed on the message route willing to act in the role denoted by the foregoing attribute **`/osci:ReceiptDemand/@s12:role.`** For interoperability reasons with Web Service implementations not able to process the receipts defined here, it may be set to "false" or not present (which is equivalent to a value of "false").

`/osci:ReceptionReceiptDemand/@qualTSPforReceipt ?`

This optional boolean attribute signals – if set to a value of "true" – a qualified timestamp for the receipt information is requested. If such a service is not available on the node the receipt is demanded from, a fault (see chapter [8.3.2]) MUST be generated to the requesting node and the message MUST be discarded.

`/osci:ReceptionReceiptDemand/@echoRequest ?`

This optional boolean attribute signals – if set to a value of "true" – the requesting node requires the retransmission of the whole message in the required receipt. In this case, the node the receipt is demanded from MUST provide the whole message in binary format in the receipt part of the response message (see chapter [8.3.2.2]). Care should be taken to use this feature with regard to caused overhead and bandwidth consumption.

If absent, this attribute defaults to a value of "false".

`/osci:ReceptionReceiptTo/wsa:ReplyTo`

This required element of type **wsa:EndpointReferenceType** denotes the endpoint, where the requestor wishes the receipt should be routed to. A ReceptionReceipt in general MUST be delivered in the SOAP body of a separate new osci:Request message, hence this EPR SHOULD be the one of the MsgBox instance of the requestor or MAY be a specialized endpoint consuming receipts. The EPR MUST contain reference properties according to chapter [6, Addressing Endpoints]. A …**/wsa:ReferenceParameters** of following value SHOULD be provided:

<osci:TypeOfBusinessScenario>
www.osci.eu/2008/common/urn/messageTypes/Receipt
</osci:TypeOfBusinessScenario>.

In case off delivering a receipt to a MsgBox instance, this is the defaulted value for separating receipt message types from other ones (see chapter [6, Addressing Endpoints]).

8.3.2 Receipt Format and Processing

8.3.2.1 Delivery Receipt

DeliveryReceipts MUST be produced immediately after successful acceptance of an incoming message of type osci:Request, if a SOAP header element **/osci:DeliveryReceiptDemand** is present in the incoming osci:Request message.

The data for this type of receipt has to be carried in the resulting SOAP response message in following SOAP header block **/osci:DeliveryReceipt:**

```
<osci:DeliveryReceipt  @wsu:Id="xs:ID"
 <osci:ReceiptInfo
  @wsu:Id="..."
  @osci:ReceiptIssuerRole=
        "http://www.osci.eu/ws/2008/05/transport/role/MsgBox" |
        "http://www.osci.eu/ws/2008/05/transport/role/Recipient"

  <wsa:MessageID>xs:anyURI</wsa:MessageID>
  <osci:MsgTimeStamps/>
  <wsa:RelatesTo/> *
  <osci:To> EPR </osci:To>
  <wsa:ReplyTo> EPR </wsa:ReplyTo>
  <wsa:From> EPR </wsa:From> ?
  <osci:RequestEcho> xs:base64Binary </RequestEcho> ?
 </osci:ReceiptInfo>
 <ds:Signature/>
</osci:Receipt>
```

Description of elements and attributes in the schema overview above:

/osci:DeliveryReceipt

Container holding the child elements receipt data …**/osci:ReceiptInfo** and a **ds:Signature** element over …**/osci:ReceiptInfo**.

/osci:DeliveryReceipt/@wsu:Id

This attribute of type **xs:ID** MUST be provided so that un-ambiguous references (i.e. for transport signature and encryption) can be made to this **/osci:DeliveryReceipt** block.

/osci:DeliveryReceipt/osci:ReceiptInfo

Container to hold the receipt details.

/osci:DeliveryReceipt/osci:ReceiptInfo/wsu:@Id

This attribute of type **xs:ID** MUST be provided; the element must be referenceable from the signature element described below.

/osci:DeliveryReceipt/osci:ReceiptInfo/osci:ReceiptIssuerRole

This element of type **xs:anyURI** MUST be provided with one of the URIs outlined above. The concrete value MUST expose the role of the receipt issuing node. If an osci:Request is targeted to a MsgBox instance, the value MUST be **"http://www.osci.eu/ws/2008/05/transport/role/MsgBox"**. If an osci:Request if targeted directly to the recipients OSCI Gateway or an osci:Response message contains a demand for a DeliveryReceipt, the value MUST be **"http://www.osci.eu/ws/2008/05/transport/role/Recipient"**.

/osci:DeliveryReceipt/osci:ReceiptInfo/wsa:MessageID

The **/wsa:MessageID** SOAP header block of the message to be receipted.

/osci:ReceptionReceipt/osci:ReceiptInfo/osci:MsgTimeStamps

The **/osci:MsgTimeStamps** SOAP header block; this element MUST be inserted after the receipting node has inserted his specific timestamps according to chapter [8.1].

/osci:DeliveryReceipt/osci:ReceiptInfo/wsa:RelatesTo *

The **/wsa:RelatesTo** SOAP header blocks of the message to be receipted.

/osci:DeliveryReceipt/osci:ReceiptInfo/osci:To

This element of type **wsa:EndpointReference** denotes the destination EPR of the message to be receipted. At least, it MUST contain the **/wsa:To** SOAP header block of this message and those SOAP header blocks attributed by **@wsa:IsReferenceParameter="1".**

/osci:DeliveryReceipt/osci:ReceiptInfo/wsa:From ?

If present in the message to be receipted, the **/wsa:From** SOAP header block of the message to be receipted.

/osci:DeliveryReceipt/osci:ReceiptInfo/wsa:ReplyTo

The **/wsa:From** SOAP header block of the message to be receipted.

/osci:DeliveryReceipt/osci:RequestEcho ?

This element MUST be included, if the demand for the receipt contains the attribute **/osci:DeliveryReceiptDemand/@echoRequest** set to a value of **"true"**. The complete incoming message MUST be placed in this element in base64Binary format.

To be able to proof what has been sent, the Initiator in this case is strongly advised to encrypt the message body for himself, too.

/osci:DeliveryReceipt/ds:Signature

A digital signature of the DeliveryReceipt according to chapter [7.2].

One **ds:Signature** child element **ds:Reference** MUST point to the element **/osci:DeliveryReceipt/ReceiptInfo** using the same-URI reference mechanism via the ID-attribute of this element.

A second **/ds:Signature/ds:Reference** element MUST point to the **/s12:Envelope/s12:Body** block of the message to be receipted using the same-URI reference mechanism via the ID-attribute of the SOAP body block.

For a DeliveryReceipt, the received SOAP body block MUST to be signed "as is". The actual server time in UTC-format MUST be provided in

/osci:DeliveryReceipt/ds:Signature/ds:Object/
xades:QualifiyingProperties/xades:SignedProperties/
xades:SignedSignatureProperties/xades/SigningTime.

If in the receipt demand SOAP header actually processed, the attribute **/osci:DeliveryReceiptDemand/@qualTSPforReceipt** is set to a value of **"true"** and can be served from this instance, the signature element MUST be extended by a *qualified timestamp over the signature itself*. For the timestamp itself, the specification [RFC3161] applies, the placement in the signature element follows [XAdES] as described in chapter [7.2.2]:

../ds:Signature/ds:Object/xades:QualifiyingProperties/
xades:UnsignedProperties /xades:UnsignedSignatureProperties/
xades:SignatureTimeStamp/xades:EncapsulatedTimeStamp

If no appropriate qualified TSP-service can be provided, a fault MUST be generated to the requestor and processing of the incoming message MUST be aborted.

Fault 8: **QualTSPServiceNotAvailable**
[Code] Sender
[Subcode] QualTSPServiceNotAvailable
[Reason] Requested qualified TSP service not provided by targeted node
The fault [Details] property MUST outline that this timestamp was requested for a DeliveryReceipt and that the message is not accepted.

If an incoming message of type osci:Request is to be receipted, the block **/osci:DeliveryReceipt** MUST be included as SOAP header in the corresponding osci:Response message.

If the message to be receipted is of type osci:Response, the block **/osci:DeliveryReceipt** MUST be positioned as SOAP body of a new osci:Request message. This osci:Request message MUST be targeted to the endpoint denoted in **/osci:DeliveryReceiptDemand/wsa:ReplyTo.** The SOAP header block **/wsa:RelatesTo** of this message MUST be supplied with the **/wsa:MessageID** SOAP header block of the message to be receipted.

8.3.2.2 Reception Receipt

If demanded by a **osci:ReceptionReceiptDemand** SOAP header of a osci:Request or osci:Response message, Reception Receipts MUST be processed after successful decryption of the SOAP body block. Depending on the concrete arrangement of roles in an OSCI endpoint implementation it may be possible that decryption of the SOAP body and processing of a ReceptionReceipt demand is decoupled from the node that accepts incoming requests respective responses (where DeliveryReceipt demands have to be processed immediately). Thus, a ReceptionReceipt is generated by Ultimate Recipient instances. For a message of type osci:Response, this is the Ultimate Recipient instance on the Initiator side.
The data for this type of receipt has to be placed into following block **/osci:ReceptionReceipt** by the receipt generating node. The underlying schema nearly the same as for a **osci:DeliveryReceipt** SOAP header block; possible attribute/element values and semantics differ in detail as described here.

```
<osci:ReceptionReceipt  @wsu:Id="xs:ID" ? >
 <osci:ReceiptInfo   @wsu:Id="..." >

   <wsa:MessageID>xs:anyURI</wsa:MessageID>
   <osci:MsgTimeStamps/>
   <wsa:RelatesTo/> *
   <osci:To> EPR </osci:To>
   <wsa:ReplyTo> EPR </wsa:ReplyTo>
   <wsa:From> EPR </wsa:From> ?
   <osci:RequestEcho> xs:base64Binary </RequestEcho> ?
 </osci:ReceiptInfo>
```

```
  <ds:Signature/>
</osci:Receipt>
```

Description of elements and attributes in the schema overview above:

/osci:ReceptionReceipt

Container holding the child elements receipt data …**/osci:ReceiptInfo** and a **ds:Signature** element over …**/osci:ReceiptInfo**.

/osci:ReceptionReceipt/@wsu:Id

This attribute of type **xs:ID** SHOULD be provided so that un-ambiguous can be made to this **/osci:ReceptionReceipt** block.

/osci:ReceptionReceipt/osci:ReceiptInfo

Container to hold the receipt details.

/osci:ReceptionReceipt/osci:ReceiptInfo/wsu:@Id

This attribute of type **xs:ID** MUST be provided; the element must be referenceable from the signature element described below.

/osci:ReceptionReceipt/osci:ReceiptInfo/wsa:MessageID

The **/wsa:MessageID** SOAP header block of the message to be receipted.

/osci:ReceptionReceipt/osci:ReceiptInfo/osci:MsgTimeStamps

The **/osci:MsgTimeStamps** SOAP header block; this element MUST be inserted after the receipting node has inserted his specific timestamps according to chapter [8.1].

/osci:ReceptionReceipt/osci:ReceiptInfo/wsa:RelatesTo *

The **/wsa:RelatesTo** SOAP header blocks of the message to be receipted.

/osci:ReceptionReceipt/osci:ReceiptInfo/osci:To

This element of type **wsa:EndpointReference** denotes the destination EPR of the message to be receipted. At least, it MUST contain the **/wsa:To** SOAP header block of this message and those SOAP header blocks attributed by **@wsa:IsReferenceParameter="1".**

/osci:ReceptionReceipt/osci:ReceiptInfo/wsa:From ?

If present in the message to be receipted, the **/wsa:From** SOAP header block of the message to be receipted.

/osci:ReceptionReceipt/osci:ReceiptInfo/wsa:ReplyTo

The **/wsa:ReplyTo** SOAP header block of the message to be receipted.

/osci:ReceptionReceipt/osci:RequestEcho ?

This element MUST be included, if the demand for the receipt contains the attribute **/osci:ReceptionReceiptDemand/@echoRequest** set to a value of **"true"**. The complete incoming message MUST be placed in this element in base64Binary format.

/osci:ReceptionReceipt/ds:Signature

A digital signature of the ReceptionReceipt according to chapter [7.2.2]. The signature MUST be generated by the Ultimate Recipient after successful decryption of the whole SOAP body block. In case a synchronous osci:Response to an osci:Request containing a ReceptionReceipt demand, this is the respective UltimateRecipient node on the Initiator side. If complete decryption of the received SOAP body is not possible, a fault MUST be generated and further message processing MUST be aborted.

Fault 9: **MsgBodyDecryptionError**

[Code] Sender
[Subcode] MsgBodyDecryptionError
[Reason] Message body decryption failed.

The fault [Details] property MAY outline – if known to the decrypting instance - the **`ds:X509IssuerSerial`** element of the certificate initially used for encryption.

One **`ds:Signature`** child element **`ds:Reference`** MUST point to the element **`/osci:ReceptionReceipt/ReceiptInfo`** using the same-URI reference mechanism via the ID-attribute of this element.

A second **`/ds:Signature/ds:Reference`** element MUST point to the element **`/s12:Envelope/s12:Body`** element of the message to be receipted using the same-URI reference mechanism via the ID-attribute of the SOAP body block. As already mentioned, the SOAP body block in advance MUST have been successfully decrypted.

The actual server time in UTC-format MUST be provided in the child element **`/xades:SigningTime`** of **`/osci:ReceptionReceipt/ds:Signature/ds:Object/xades:QualifiyingProperties/xades:SignedProperties/xades:SignedSignatureProperties.`**

If in the receipt demand SOAP header actually processed, the attribute **`/osci:ReceptionReceiptDemand/@qualTSPforReceipt`** is set to a value of **`"true"`** and can be served from this instance, the signature element MUST be extended by a *qualified timestamp over the signature itself*. For the timestamp itself, the specification [RFC3161] applies, the placement in the signature element follows [XAdES] as described in chapter [7.2.2]:

```
.../ds:Signature/ds:Object/xades:QualifiyingProperties/
        xades:UnsignedProperties/
            xades:UnsignedSignatureProperties/
              xades:SignatureTimeStamp/xades:EncapsulatedTimeStamp
```

If no appropriate qualified TSP-service can be provided, a fault MUST be generated to the requestor instead of the ReceptionReceipt, processing of the incoming message MAY proceed (subject to policy to be defined for the concrete endpoint). See fault **QualTSPServiceNotAvailable** as defined in chapter [8.3.2.1]; the fault [Details] property MUST outline that this timestamp was requested for a ReceptionReceipt and if further message processing takes place or not.

The block **`/osci:ReceptionReceipt`** MUST be positioned as SOAP body of a new osci:Request message. This osci:Request message MUST be targeted to the endpoint denoted in **`/osci:ReceptionReceiptDemand/wsa:ReplyTo`**. The SOAP header block **`/wsa:RelatesTo`** of this message MUST be supplied with the **`/wsa:MessageID`** SOAP header block of the message to be receipted.

8.3.2.3 Additional Receipt/Notification Demand fault processing Rules

As fault occurrence is imaginable while processing receipt demands, it must be foreseen to communicate those faults to the requestor of a receipt. As far as a receipt has to be delivered directly in the SOAP header of a response to a request in the same http-connection, such a fault occurrence is directly communicated to the requestor by the general SOAP/OSCI fault processing mechanisms and the message is discarded. **No receipt SOAP header block MUST be build up and inserted in the response in this case.**

For receipts which have to be processed asynchronous mode and/or delivered in a separate osci:Request message, the receipt requestor has to be informed about possible fault occurrence asynchronously. This MUST be done by placing the fault information in the body of an osci:Request instead of the receipt block and delivered to the same endpoint the receipt message is expected.

If the message to be receipted carries a **wsa:FaultTo** SOAP header block, this is the EPR the osci:Request message carrying the fault MUST be targeted to. If this header is absent or – if present and carrying a value of **http://www.w3.org/2005/08/addressing/anonymous** in **wsa:FaultTo/Address**, it MUST be targeted to the endpoint denoted in **/osci:ReceptionReceiptDemand/wsa:ReplyTo/Address**. The according **wsa:ReferenceParameters** SOAP header block MUST be

```
<osci:TypeOfBusinessScenario wsa:IsReferenceParameter="true">
    www.osci.eu/2008/common/urn/messageTypes/Fault
</osci:TypeOfBusinessScenario>
```

The SOAP header block **/wsa:RelatesTo** of this message MUST be supplied with the **/wsa:MessageID** SOAP header block of the message to be receipted.

ReceptionReceipts and FetchedNotification in general have to be delivered in asynchronous mode. If the request for these doesn't indicate a valid address they can be successfully targeted to, standard SOAP addressing error handling applies. It is strongly advised, that these errors SHOULD be logged at the node producing the requested receipt/notification; follow-up of this situation is up to the operating policies[19].

8.3.2.4 Receipt Signature Validation

Receipt signatures MUST be verified by receipt consuming nodes. If signature verification fails, a fault MUST be generated and be made available to the Source Application instance initially triggering the corresponding receipt demand. Fault delivery in this case is a matter of implementation.

Fault 10: **SignatureOfReceiptInvalid**	
[Code]	Sender
[Subcode]	SignatureOfReceiptInvalid
[Reason]	Receipt signature verification failed.

The fault [Details] property SHOULD outline the concrete verification failure. It is on behalf of the Source Application to handle this situation.

8.3.3 Fetched Notification

To demand a FetchedNotification from a recipient MsgBox instance where the message is relayed, following SOAP header block MUST be provided in an osci:Request message:

```
<osci:FetchedNotificationDemand @wsu:Id="..." ?
   @s12:role="http://www.osci.eu/ws/2008/05/transport/role/MsgBox" >
  <wsa:ReplyTo>wsa:EndpointReference</wsa:replyTo>
</osci:FetchedNotificationDemand>
```

Description of elements and attributes in the schema overview above:

/osci:FetchedNotificationDemand

Header block contain the demand.

/osci:FetchedNotificationDemand/@wsu:Id

For ease of referencing this SOAP header block from WS Security SOAP header elements, this attribute of type **wsu:Id** SHOULD be provided.

/osci:FetchedNotificationDemand/@s12:role

[19] Those should be made available online for all possible communication partners. Details are not addressed by this document.

This attribute of type **xs:anyURI** MUST be provided with the URI outlined above. Only nodes acting in the role MsgBox are addressed by this type of demand.

/osci:ReceiptTo/wsa:ReplyTo

This required element of type **wsa:EndpointReferenceType** denotes the endpoint, where the requestor wishes the notification should be routed to. As FetchedNotifications can only be delivered in the SOAP body of a separate new message, this EPR SHOULD be the one of the MsgBox instance of the requestor or MAY be a specialized endpoint consuming notifications. The EPR MUST contain reference properties according to chapter [6, Addressing Endpoints]. A .../**wsa:ReferenceParameters** of following value SHOULD be provided: **<osci:TypeOfBusinessScenario>www.osci.eu/2008/common/urn/messageTypes/Notification/>.** In case of delivering a receipt to a MsgBox instance, this is the defaulted value for separating notification message types from other ones (see chapter [6, Addressing Endpoints]).

A SOAP header **/osci:FetchedNotificationDemand** MUST be processed by a node acting in the role of MsgBox when the message is pulled the first time by the Recipient of the message. It MUST be delivered in a separate message to the endpoint denoted in the appropriate demand. They MUST only be produced by MsgBox instances. The **/osci:FetchedNotification** block is positioned in the body of such a message, other body parts MUST NOT be included.

Syntax for messages to deliver FetchedNotifications:

```
<s12:Envelope ...>
 <s12:Header ...>
  ...
   <wsa:Action>
    www.osci.eu/2008/transport/urn/messageTypes/Notification
   </wsa:Action>
   <wsa:MessageID>xs:anyURI</wsa:MessageID>
   <wsa:RelatesTo>xs:anyURI</wsa:RelatesTo>
   <wsa:To>xs:anyURI</wsa:To>
    <osci:TypeOfBusinessScenario @wsa:IsReferenceParameter="1">
     "www.osci.eu/2008/common/urn/messageTypes/Notification"/>
    </osci:TypeOfBusinessScenario>
   ...
  </s12:Header>
 <s12:Body>
  <osci:FetchedNotification> @wsu:Id="..." ?>
      <osci:FetchedTime> xs:dateTime </osci:FetchedTime>
    <wsa:MessageID>xs:anyURI</wsa:MessageID>
     <wsa:To> esa:Address </wsa:To>
    <wsa:From> EPR </wsa:From>
  </osci:FetchedNotification>
</s12:Body>
</s12:Envelope>
```

Description of elements and attributes in the schema overview above:

/s12:Envelope/s12:Header/wsa:Action

The value indicated herein MUST be used for that URI.

/s12:Envelope/s12:Header/wsa:MessageID

The message MUST carry a unique WS-Addressing MessageID.

/s12:Envelope/s12:Header/wsa:RelatesTo

The message MUST carry the WS-Addressing MessageID for the message a FetchedNotification was requested for.

/s12:Envelope/s12:Header/wsa:To

The address of the destination endpoint which was stated in the EPR of the request header element **/osci:FetchedNotificationTo/wsa:ReplyTo/wsa:Address** of the request message.

/s12:Envelope/s12:Header/osci:TypeOfBusinessScenario

This is the instantiation of **/wsa:ReferenceParameters** bound to this EPR. It MUST be taken from the request header element **/osci:FetchedNotificationTo/wsa:ReplyTo/wsa:ReferenceParameters** of the request message.

/s12:Envelope/s12:Header/osci:TypeOfBusinessScenario/ @wsa:IsReferenceParameter

Following WS-Addressing, the element MUST be attributed with **@wsa:IsReferenceParameter="1"**

/s12:Envelope/s12:Body/osci:FetchedNotification

Container holding the FetchedNotification.

/osci:Receipt/osci:FetchedNotification/osci:FetchedTime

This element of type **xs:dateTime** MUST be set to the actual server time instance in UTC format when the MsgBox node processes the FetchedNotification demand (message first time pulled from recipient).

/s12:Envelope/s12:Body/osci:FetchedNotification/wsa:MessageID

The .../**wsa:MessageID** of the message to give a FetchedNotification for.

/s12:Envelope/s12:Body/osci:FetchedNotification/wsa:To

The .../**wsa:To** element of the message to give a FetchedNotification for.

/s12:Envelope/s12:Body/osci:FetchedNotification/wsa:From

The .../**wsa:From** header element of the message to give a FetchedNotification for.

8.4 X.509-Token Validation on the Message Route

A custom SOAP header is defined here for carrying X.509-Certificates and details per usage instance in the referred message body block parts.

Certificate validation processing SOAP nodes MUST enrich the message SOAP header block with the gathered certificate validation results and – for processing optimization purposes – mark those usage instances of a certificate as "checked", if validation could be processed successfully.

An XML-Syntax to carry validation results is defined by XKMS 2/XKISS [XKMS], which is incorporated here. The **/xkms:ValidateResult** specified in XKMS includes original validation responses from CAs like OCSP-Responses and CRLs. In addition to [XKMS], extensions are defined to satisfy requirements coming out the German signature law/directive regarding certificate validation. These extensions are optional in general, but MUST be provided from OSCI service providers in Germany.

Ultimate Recipients of messages MAY rely on the validation information thus once included in the message body. As at least the inner CA-Responses are verifiable, as they are carrying signatures of respective validation responders (OCSP, CRL…). In general, it's up to each node or endpoint on the message route to rely on the validation information found in the message or to initiate revalidation of used certificates following own needs und trust relations.

This specification enforces no rules how a node serving certificate validation obtains certificate validation results. It SHOULD be preferred to use the services of a trusted XKMS/XKISS responder instance, like this a **/xkms:ValidateResult** can easily be gathered by the corresponding **/xkms:ValidateRequest**. If the used XKMS/XKISS responder is designed as a relay bridging links

to all relevant CAs concerning the overall requirements of a concrete OSCI based communication network , the burden of administrating CA-links and serving further protocols for those links is delegated to the XKMS/XKISS responder provider.

If using a XKMS responder, it is advisable to use the advantage of compound validation request offered by the XKMS/XKISS protocol. All validation requests for all usage instances of the certificates exposed in the **`/osci:X509TokenContainer`** custom SOAP header block MAY be combined in one compound request, which leads to a corresponding compound response. See [XKMS] for further details.

8.4.1 X.509-Token Container

This chapter describes this optional custom header to carry those certificates. In addition to the token themselves, following information is carried, which has to be provided by Source- / Target Applications per token-usage:

- Where a certificate is used in the body (by IDREF); information may be useful at recipient side when parsing a message after SOAP body block decryption and grouping together derived body block parts with their respective certificates/validation results (at least, validation of signatures contained in the body SHOULD happen now)
- Application time instant (this is the time instant a certificate must be proven as valid)
- Possibility to indicate forced online OCSP request to downstream validation service nodes (force bypassing possible cacheing of once gained OCSP responses).

While processing the validation, such a node supplies following additional information:

- A reference to the corresponding **`/xkms:ValidateResult`** per usage instance
- An indicator "validated" if all usage instance of a token have successfully been validated (note: only indication the fact of validation, not the result!)
- An indicator "validation completed" when all usage instances of all carried token have successfully been validated.

As under certain circumstances it may be, that a certificate validations serving node is not able to gather all needed **`/xkms:ValidateResult(`**s) completely, the latter two indicators only serve for processing optimization – they can be used to avoid iterating through the X509 token container and checking for outstanding **`/xkms:ValidateResult`**(s) by downstream nodes / endpoints on the message route.

Syntax for an optional **`/osci:X509TokenContainer`**:

```
<osci:X509TokenContainer validateCompleted=("true" | "false")? >
  <osci:X509TokenInfo Id="xs:ID"
            validated=("true" | "false")? >
    <ds:X509Data>
      <ds:X509Certificate>
    </ds:X509Data>
    <osci:TokenApplication
      ocspNoCache=("true" | "false")? >
      validateResultRef="xs:IDREF" ? >
        <osci:TimeInstant>xs:dateTime</osci:TimeInstant>
        <osci:MsgItemRef>xs:IDREF</osci:MsgItemRef>
    </osci:TokenApplication> +
  </osci:X509TokenInfo> +
</osci:X509TokenContainer>
```

Description of elements and attributes in the schema overview above:

`/osci:X509TokenContainer ?`

Optional SOAP header block containing the X.509-Certificates which SHOULD be validated by a node on the message route with validation capabilities.

This container SHOULD be provided by a Source Application together with the payload to be placed in the message body block at OSCI gateway entry point towards applications. If present in an incoming message, it MUST be provided to the addressed Target Application by the recipients OSCI gateway.

/osci:X509TokenContainer/@validateCompleted ?

This optional boolean attribute MUST be provided with a value of "true" by a validation processing node, when processing was successfully passed for all application instances of all contained items **/osci:X509TokenInfo**. It MUST NOT provided with a value of "true" if this condition is false – i.e. only partially successful validation processing. It MUST NOT be provided or changed by other logical instances than validation processing nodes.

/osci:X509TokenContainer/osci:X509TokenInfo +

If an **/osci:X509TokenContainer** is present, it MUST contain at least one item of this type; content description follows here:

/osci:X509TokenContainer/osci:X509TokenInfo/@Id

This mandatory attribute of type **xs:ID** MUST be provided. As the whole **/osci:X509TokenContainer** is initially to be generated by a Source Application instance, the value must be a UUID; the UUID-value MUST NOT start with a character unlike the **xs:ID** production rules and SHOULD therefore be preceded by a string of "uuid:". This attribute MUST NOT be provided or changed by other logical instances than Source Applications.

/osci:X509TokenContainer/osci:X509TokenInfo/@validated ?

This optional boolean attribute of type **xs:ID** MUST be provided with a value of "true" by a validation processing node, when processing was successfully passed for all application instances of this item **/osci:X509TokenInfo**. It MUST NOT provided with a value of "true" if this condition is false – i.e. only partially successful validation processing. It MUST NOT be provided or changed by other logical instances than validation processing nodes.

/osci:X509TokenContainer/osci:X509TokenInfo/ds:X509Data

The X.509-Token of type **ds:Data** MUST be provided here by the Source Application instance. Other sub-elements than **X509Certificate** foreseen in **ds:X509Data** MUST NOT be provided.

/osci:X509TokenContainer/osci:X509TokenInfo/ds:X509Data/ds:X509Certificate

Sub-element .../**ds:509Certificate** MUST be provided. It MUST NOT be provided or changed by other logical instances than Source Applications.

/osci:X509TokenContainer/osci:X509TokenInfo/osci:TokenApplication

A Source Application MUST initially provide this container containing application details of the X.509-Token.

/osci:X509TokenContainer/osci:X509TokenInfo/osci:TokenApplication/ @ocspNoCache ?

This optional boolean attribute MUST be provided with a value of "true" by the Source Application instance, when the downstream validation service node shall be forced bypassing possible cacheing of OCSP responses while validating this certificate. If not provided with a value of "true", a validation service node MAY use cacheing mechanisms to build up validation results. It MUST NOT be provided or changed by other logical instances than a Source Application instance.

/osci:X509TokenContainer/osci:X509TokenInfo/osci:TokenApplication/ @validateResultRef ?

Validation processing nodes MUST provide an **xs:IDREF** here when processing was successfully passed for this instance of **/osci:X509TokenInfo/TokenApplication**. It must point to the related **/xkms:ValidateResult** header child element (see next chapter). It MUST NOT be provided or changed by other logical instances than validation processing nodes. If present, this attribute indicates, that this instance of **/osci:X509TokenInfo/osci:TokenApplication** is validated.

/osci:X509TokenContainer/osci:X509TokenInfo/osci:TokenApplication/ osci:TimeInstant

This element of type **xs:dateTime** MUST be provided by the Source Application instance and carry the token application time instant. This time instant MUST be taken as validation time instant by the validation processing node (see next chapter). It MUST NOT be provided or changed by other logical instances than Source Applications.

/osci:X509TokenContainer/osci:X509TokenInfo/osci:TokenApplication/ osci:MsgItemId

This element of type **xs:IDREF** MUST be provided by the Source Application instance and carry a reference to the cryptographic element in the message body where the token was used. It MUST NOT be provided or changed by other logical instances than Source Applications.

8.4.2 X.509-Token Validation Results

SOAP nodes which are willing and able processing validation for X.509-Certificates contained in the **/osci:X509TokenContainer** SOAP header block MUST insert the processing result in SOAP header blocks /**xkms:CompoundResult** containing one or more **/xkms:ValidateResult** elements conformant to the part XKISS of the XKMS specification. See [XKMS] for details, whereby following profiling applies here:

R1100: Validation results MUST be signed by the generating instance. This MAY be a XKMS-Responders involved or – if no dedicated XKMS-Responder is used – the node generating the header block **/xkms:CompundResult** containing **the /xkms:ValidateResult** elements. Hence, the element **/xkms:CompoundResult/ds:Signature** MUST be present. The subordinate signature elements **/xkms:ValidateResult/ds:Signature** SHOULD be omitted.

R1120: For nodes consuming the validation results, it MUST be able to establish trust to the validation results generating node through the certificate used for this signature. If no trust can be established, these nodes MUST ignore the affected header block **/xkms:CompoundResult** and MUST revalidate the affected certificates using a service trusted by this node.

R1130: Nodes consuming the validation results MUST validate the signature of the **/xkms:CompoundResult.** If signature validation fails, this fact MUST be logged as a security error including the affected header block. This header block MUST be ignored, the affected certificates using a service trusted by this node.

For XKMS messages an abstract extension point **xkms:MessageExtension** is foreseen to carry additional information. German regulations as well as EU-wide efforts for alingnment of interoperable use of electronic signatures require detailed information on certificate quality, validity status, used algorithm suitability and the validation process itself. Thus, a **/xkms:ValidateResult** SHOULD contain an extension block **/xkmsEU,** XML namespace **http://www.lsp.eu/2009/04/xkmsExt#** as defined in chapter 5.3 of [XKMSEU] [20].

[20] These extensions are subject to alignement in the context of running EU-wide "Large Scale Pilot" (lsp) projects. Concrete work on these issues is done by the procject PEPPOL, see www.peppol.eu. One goal is a common

8.4.3 Verification of XKMS Validate Result Signatures

Signatures of **`xkms:CompoundResult`** header elements MUST be verified by nodes consuming these header elements during the process of Content Data signatures. If signature verification fails, a fault MUST be generated and be made available to the instance validating Content Data signatures. Affected **`xkms:CompoundResult`** header element MUST NOT be consumed, certificate validation processing MUST be reprocessed by means out of scope of this specification. It is strongly RECOMMENDED to log this security error. Fault delivery is an implementation matter.

Fault 11: **SignatureOfValidateResultInvalid**	
[Code]	Sender
[Subcode]	SignatureOfValidateResultInvalid
[Reason]	Verification failed for XKMS validate result

The fault [Details] property SHOULD outline the concrete verification failure.

8.5 General Processing of Custom Header Faults

Nodes a message is targeted to MUST validate the structure of the OSCI extension headers. If syntactically invalid or not conformant to this specification, the message MUST be discarded and following fault MUST be generated:

Fault 12: **MsgHeaderStructureSchemaViolation**	
[Code]	Sender
[Subcode]	MsgHeaderStructureSchemaViolation
[Reason]	On ore more OSCI header violate schema definitions

More information SHOULD be given in the fault [Details] property, at least the concrete header element the error was located in form of an XPath expression relative to the **`s12:Envelope`** element.

XKMS-Responder infrastructure in the EU member states. The namespace has to be seen as preliminary. The concrete XKMS extension structure is subject to further refinement in 2009.

9 Constituents of OSCI Message Types

For all OSCI message types, the SOAP header and body block assemblies as well as their respective transport signature/transport encryption requirements are defined in this chapter.

For a quick overview, constituents of each message type are illustrated in diagrams.

In general, most header and body blocks are marked to be encrypted optionally. These blocks MUST be included in the transport encryption according to chapter [7], if no symmetric binding (transport over https) is used or the network between nodes involved in the message transport is secured by other precautions.

9.1 osci:Request

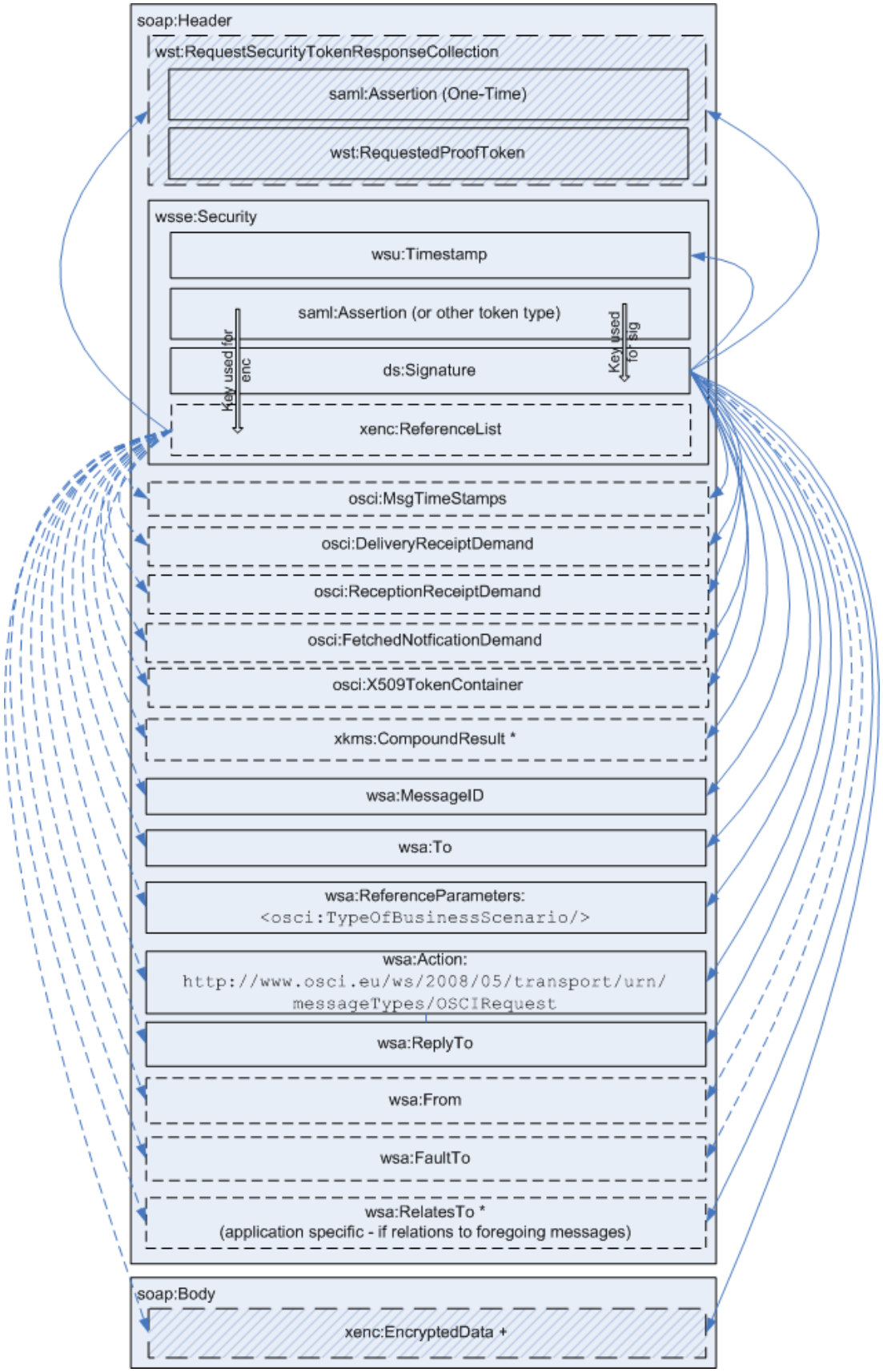


Figure 8: osci:Request header and body block assembly

SOAP header blocks:

/wst:RequestSecurityTokenResponseCollection ?

This header block carries the SAML token which is needed for asynchronously delivery of receipts and notification (see chapter [7.5.5] for details). It MUST only be present, when these receipts and/or notification are required from a node in a foreign TD.

/wsse:Security

This header block MUST be present, carrying message protection data and Initiator authentication and authorization information items according the security policy of the node the message is targeted to. See chapter [7.1] for details.

/osci:MsgTimeStamps ?

This optional header block MUST only be set by the Initiator, if he wishes to supply a …**/osci:ObsoleteAfter** date in here. This header block MUST be set by a MsgBox instance and MAY be set – if not yet present - by a Recipient instance. This header block MUST always be relayed. See chapter [8.1] for details.

/osci:DeliveryReceiptDemand ?

This optional header block MUST only be set by the Initiator, if he wishes to receive a DeliveryReceipt in the backchannel response message. This header block MUST be removed from the message by the node processing it. See chapter [8.3.1.1] for details.

/osci:ReceptionReceiptDemand ?

This optional header block MUST only be set by the Initiator, if he wishes to receive a ReceptionReceipt. This header block MUST be removed from the message by the node processing it. See chapter [8.3.1.2] for details.

/osci:FetchedNotificationDemand ?

This optional header block MUST only be set by the Initiator, if he wishes to receive a FetchedNotification. This header block MUST only be processed by a MsgBox node instance and MUST be removed from the message after processing it. See chapter [8.3.3] for details.

/osci:X509TokenContainer ?

This optional header block SHOULD by provided by the Initiator, if he wishes to enable certificate validation on the message route. This header block MUST always be relayed. See chapter [8.4.1] for details.

/xkms:CompoundResult ?

This optional header block MUST by provided by nodes processing the header block **/osci:X509TokenContainer**. This header block containing **/xkms:ValidateResult** elements MUST always be relayed. See chapter [8.4.2] for details.

/wsa:*

All WS-Addressing headers MUST (if in continuous blocks) /MAY (if in dashed blocks) be supplied by the Initiator and MUST always be relayed. See chapter [6.1.2] for details.

SOAP body:

Carries the request message ContentData, generally MUST be encrypted by the Source Application or Initiator for the Ultimate Recipient.

9.2 osci:Response

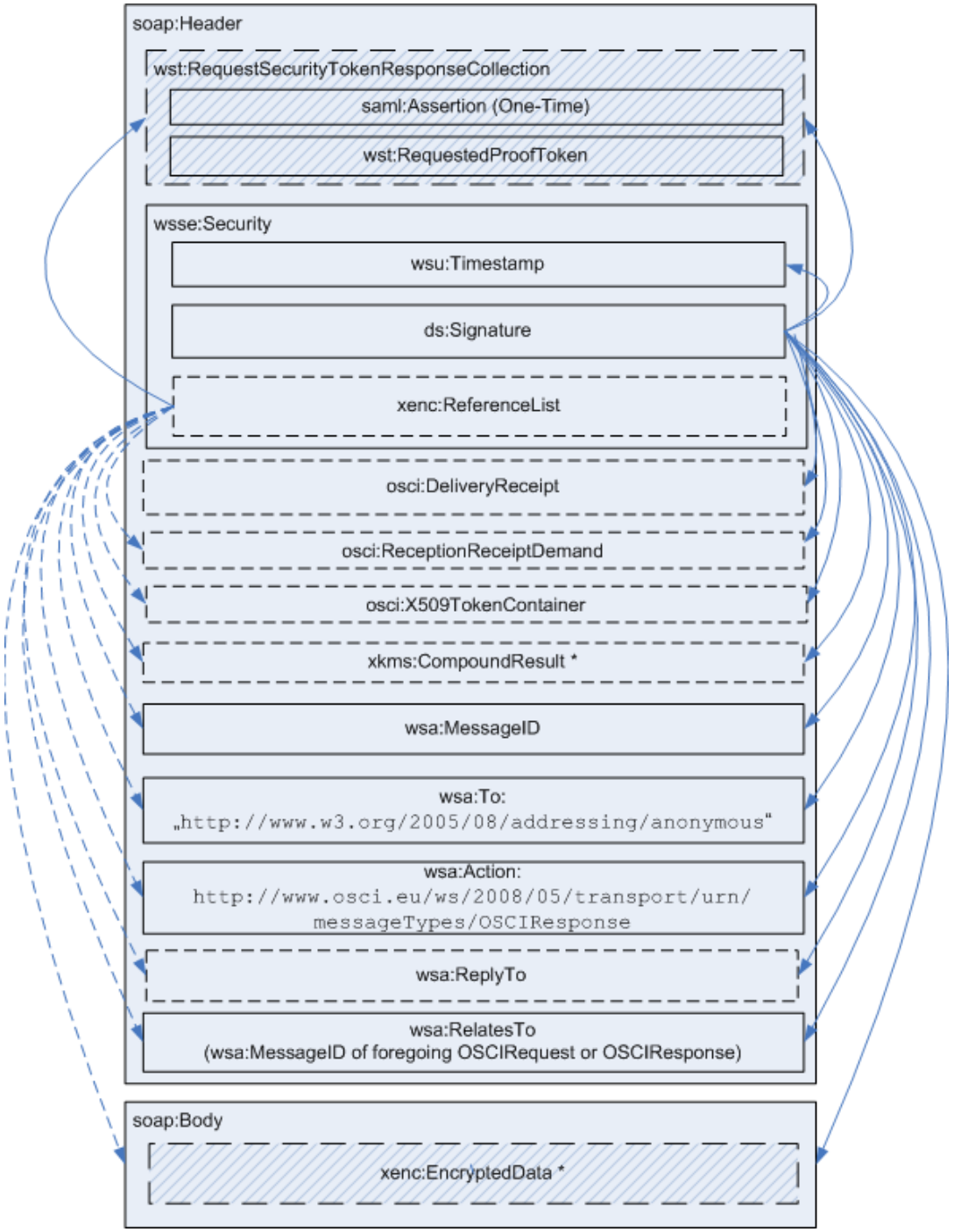


Figure 9: osci:Response header and body block assembly

SOAP header blocks:

`/wst:RequestSecurityTokenResponseCollection ?`

This header block carries the SAML token which is needed for asynchronously delivery of receipts and notification (see chapter [7.5.5] for details). It MUST only be present, when these receipts and/or notification are required from a node in a foreign TD.

/wsse:Security

This header block MUST be present, carrying message protection data. See chapter [7.1] for details.

/osci:DeliveryReceipt ?

This optional header block MUST be provided by the responding endpoint, if a demand for a DeliveryReceipt is present in the corresponding request. This header block MUST not be discarded or changed on the message route. See chapter [8.3.2] for details.

/osci:ReceptionReceiptDemand ?

This optional header block MUST only be set by the responding Recipient, if he wishes to receive a ReceptionReceipt for the response message. This header block MUST NOT be set by a MsgBox instance. This header block MUST be removed from the message by the node processing it. See chapter [8.3.1.2] for details.

/osci:X509TokenContainer ?

This optional header block SHOULD by provided by the responding Recipient, if he wishes to enable certificate validation on the message route. This header block SHOULD NOT be set by a MsgBox instance. This header block MUST always be relayed. See chapter [8.4.1] for details.

/xkms:CompoundResult ?

This optional header block MUST by provided by nodes processing the header block **/osci:X509TokenContainer**. This header block block containing **/xkms:ValidateResult** elements MUST always be relayed. See chapter [8.4.2] for details.

/wsa:*

All WS-Addressing headers MUST (if in continuous blocks) /MAY (if in dashed blocks) be supplied by the resending endpoint and MUST always be relayed. See chapter [6.1.2] for details.

SOAP body:

May carry the response message ContentData in case of point-to-point scenarios. If present, it generally MUST be encrypted by the Target Application or Recipient for the Initiator. If an error occurred, a fault message is placed here instead.

9.3 MsgBoxFetchRequest

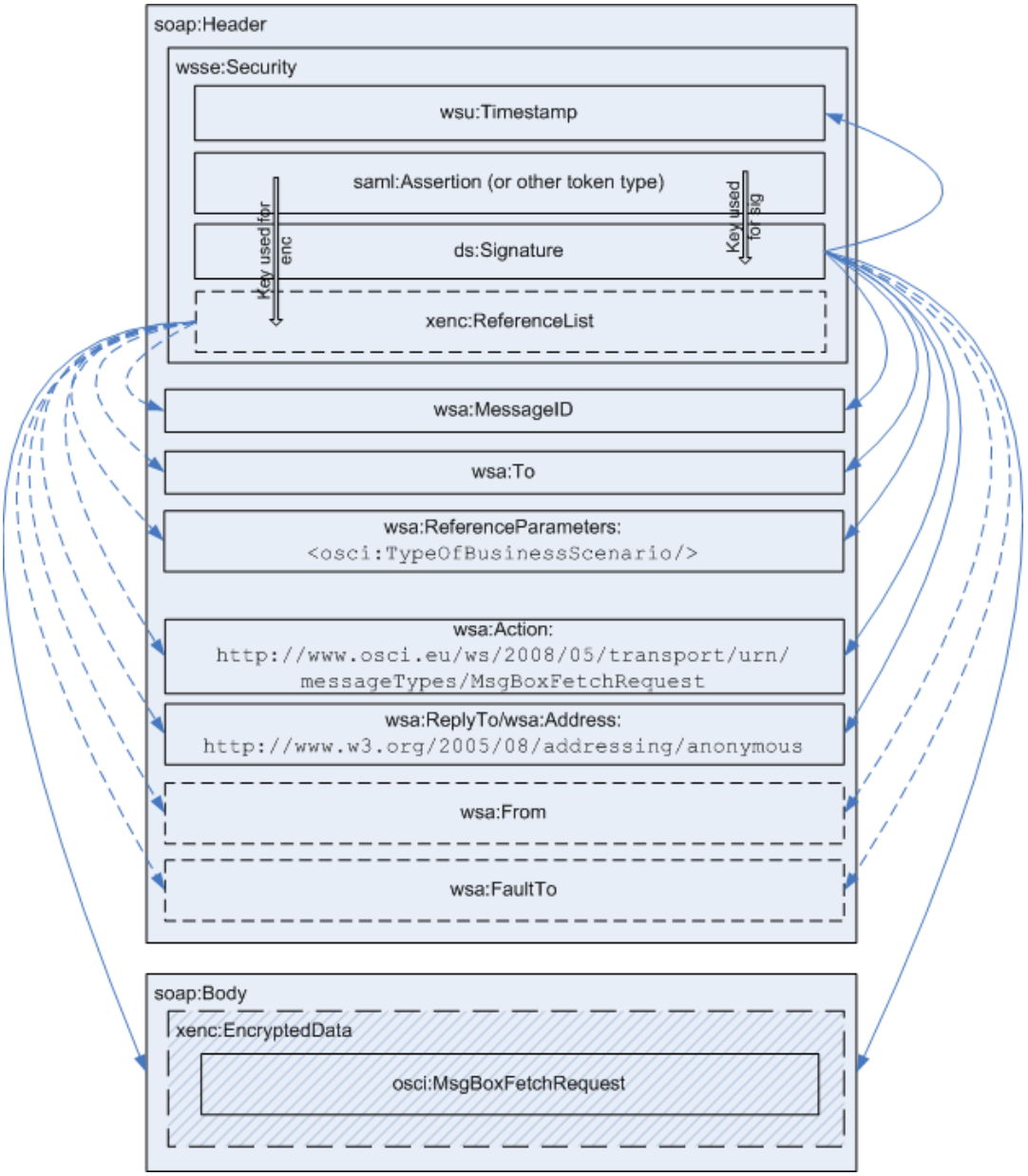


Figure 10: MsgBoxFetchRequest header and body block assembly

SOAP header blocks:

`/wsse:Security`

This header block MUST be present, carrying message protection data and requestor (MsgBox owner in this case) authentication and authorization information items according the security policy MsgBox instance. See chapter [7.1] for details.

`/wsa:*`

All WS-Addressing headers MUST (if in continuous blocks) /MAY (if in dashed blocks) be supplied by the Initiator. See chapter [6.1.2] and [8.2.1] for details.

SOAP body:

Carries the details of the MsgBoxFetchRequest, generally MUST be transport encrypted. See chapter [8.2.1] for details.

9.4 MsgBoxStatusListRequest

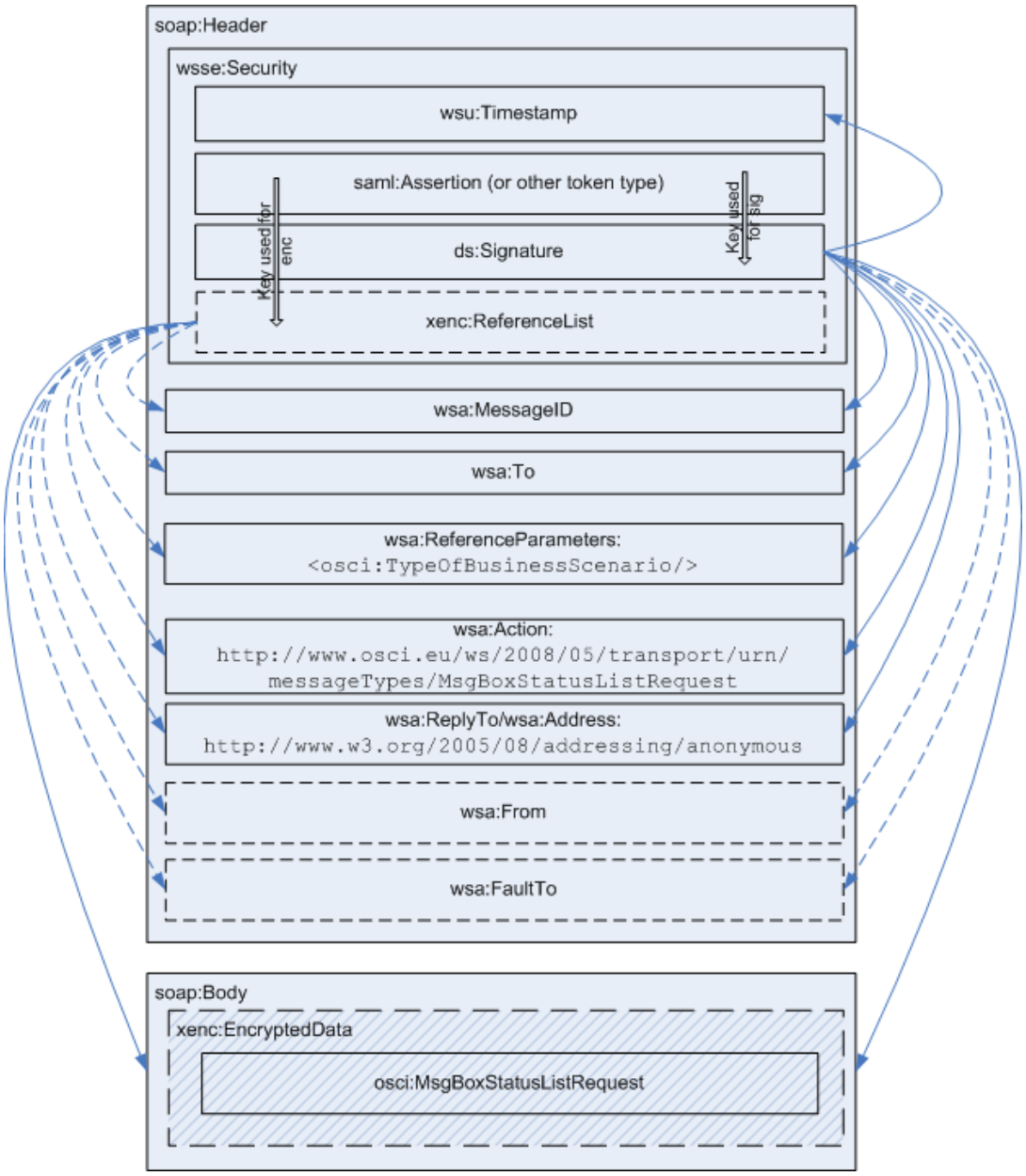


Figure 11: MsgBoxStatusListRequest header and body block assembly

SOAP header blocks:

`/wsse:Security`

This header block MUST be present, carrying message protection data and requestor (MsgBox owner in this case) authentication and authorization information items according the security policy MsgBox instance. See chapter [7.1] for details.

`/wsa:*`

All WS-Addressing headers MUST (if in continuous blocks) /MAY (if in dashed blocks) be supplied by the Initiator. See chapter [6.1.2] and [8.2.2] for details.

SOAP body:

Carries the details of the MsgBoxFetchRequest, generally MUST be transport encrypted. See chapter [8.2.2] for details.

9.5 MsgBoxResponse

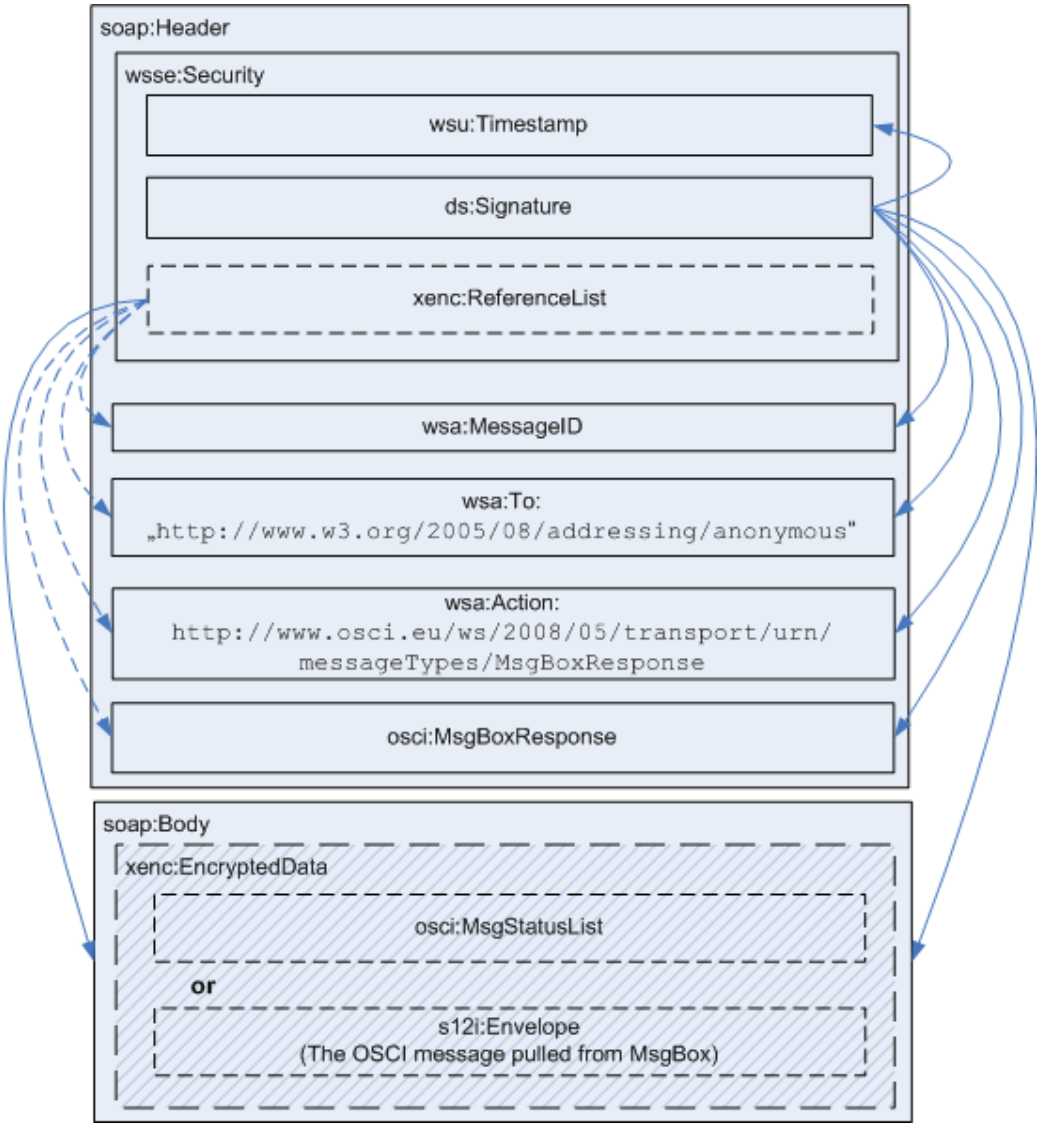


Figure 12: MsgBoxResponse header and body block assembly

SOAP header blocks:

`/wsse:Security`

This header block MUST be present, carrying message protection data. See chapter [7.1] for details.

`/wsa:*`

All WS-Addressing headers MUST (if in continuous blocks) /MAY (if in dashed blocks) be supplied by the Initiator. See chapter [6.1.2] and [8.2.3] for details.

`/osci:MsgBoxResponse`

This header carrying status information concerning the actual message box access MUST be set by the resending MsgBox instance. See chapter [8.2.3] for details.

SOAP body:

Carries the requested message status list or the message fetched from the MsgBox – depending on the initial request. It generally MUST be transport encrypted. See chapter

[8.2.3.1] and [8.2.3.2] for details. If an error occurred, a fault message is placed here instead.

9.6 MsgBoxGetNextRequest

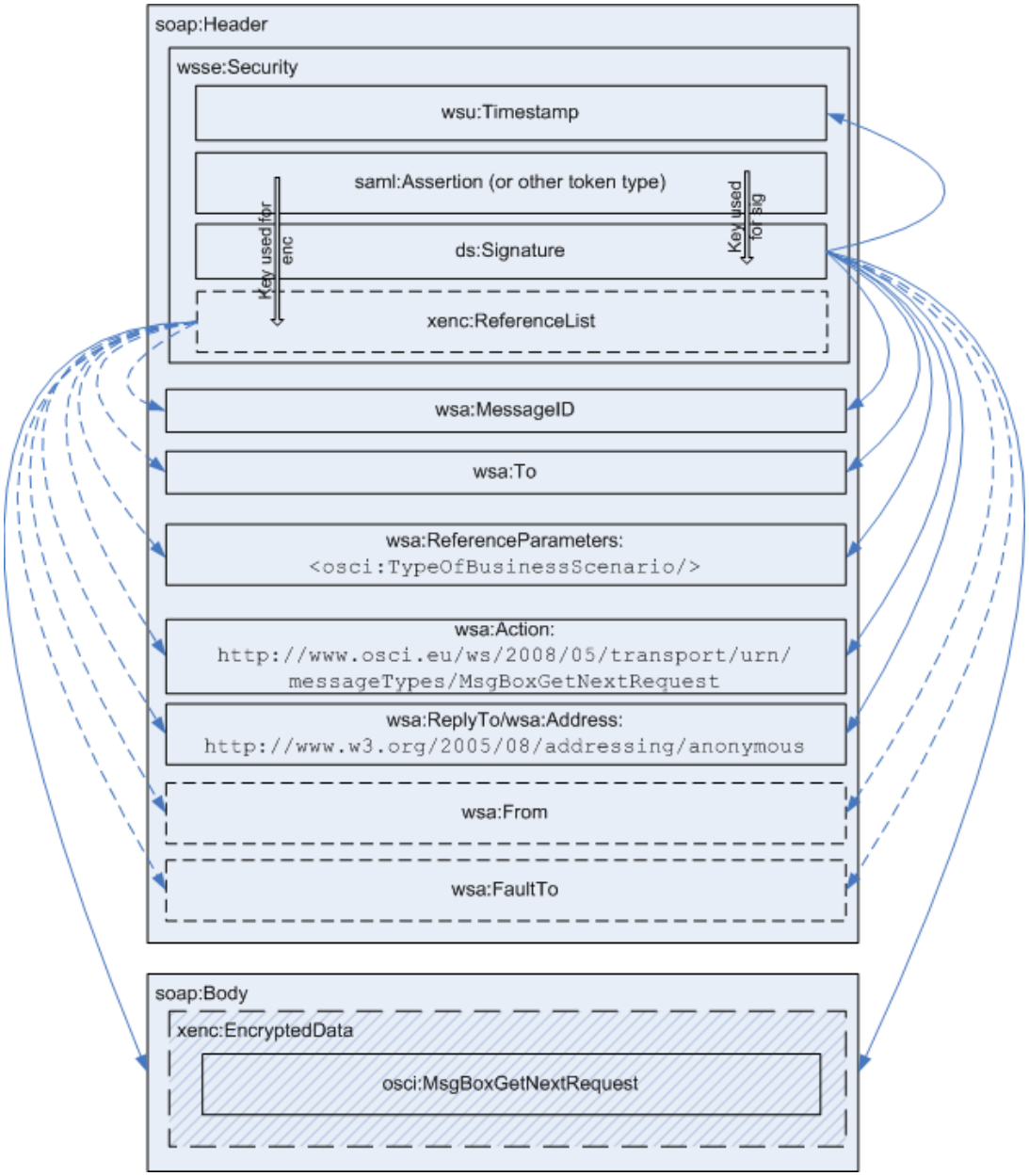


Figure 13: MsgBoxGetNextRequest header and body block assembly

SOAP header blocks:

`/wsse:Security`

This header block MUST be present, carrying message protection data and requestor (MsgBox owner in this case) authentication and authorization information items according the security policy MsgBox instance. See chapter [7.1] for details.

`/wsa:*`

All WS-Addressing headers MUST (if in continuous blocks) /MAY (if in dashed blocks) be supplied by the Initiator. See chapter [6.1.2] and [8.2.4] for details.

SOAP body:

Carries the details of the MsgBoxGetNextRequest, generally MUST be transport encrypted. See chapter [8.2.4] for details.

9.7 MsgBoxCloseRequest

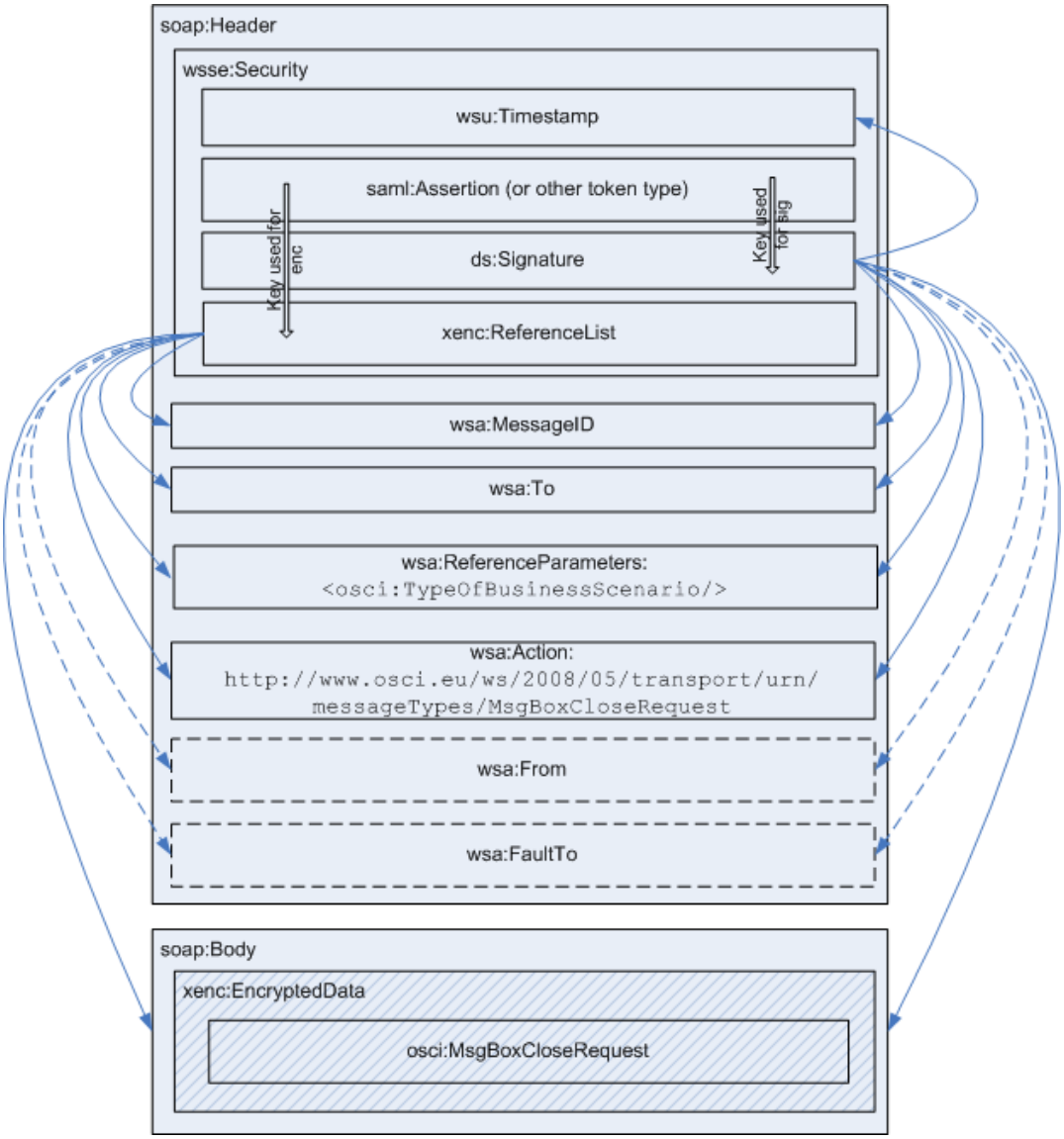


Figure 14: MsgBoxClose header and body block assembly

SOAP header blocks:

`/wsse:Security`

This header block MUST be present, carrying message protection data and requestor (MsgBox owner in this case) authentication and authorization information items according the security policy MsgBox instance. See chapter [7.1] for details.

`/wsa:*`

All WS-Addressing headers MUST (if in continuous blocks) /MAY (if in dashed blocks) be supplied by the Initiator. See chapter [6.1.2] and [8.2.5] for details.

2482 SOAP body:

2483 Carries the details of the MsgBoxCloseRequest, generally MUST be transport encrypted.
2484 See chapter [8.2.5] for details.

10 Policies and Metadata of Communication Nodes and Endpoints

10.1 General usage of Web Service Description Language

The Web Service Description Language (WSDL) provides a broadly-adopted foundation on which interoperable Web Services can be build. WS-Policy Framework [WSPF] and WS-Policy Attachment [WSPA] collectively define a framework, model and grammar for expressing the requirements, and general characteristics of entities in an XML Web Services-based system.

In general, endpoint properties and requirements MUST be described in machine readable form of WSDLs and policies. For sake of interoperability with currently available implementations of the WS-Stack, this specification restricts to Web Service Description Language 1.1 [WSDL11].

This specification does not assume a mandatory mechanism how WSDLs of endpoints must be made available. To facilitate retrieval and online exchange of WSDLs, they SHOULD be exposed in appropriate directories OSCI communication networks; the base established mechanism to access a WSDL of a concrete Web Service endpoint is a http(s) GET-Request in the form

`http(s)://endpoint-url?WSDL.`

Conformant implementations SHOULD at least support this mechanism. The specification WS Metadata Exchange [WSMEX] describes a more sophisticated way to encapsulate services metadata and a protocol to retrieve it. It allows the client to interact with the service automatically, fetch all relevant metadata and aids the client in self-configuring. Support of WS Metadata Exchange is strongly RECOMMENDED.

NOTE on WSDL/Policy integrity: Policies and WSDL-Files MUST be secured by digital signatures to allow detection of possible corruptions. Unfortunately, there is no standard format and placement defined so far by the WS-Policy Framework for adequate digital signatures, what obviously results in the lack of integrity check mechanisms in known framework implementations when accessing policies and WSDL-Files. An appropriate specification and recommendation for implementors will be published by the OSCI Steering Office mid 2009 after finishing actually running tests on solution variants addressing this issue.[21]

Endpoints are not forced to expose their properties and requirements in form of online available and machine readable WSDLs and/or policies. Developers may exchange this information on informal basis out of scope of this specification (i.e. word-of-mouth, documentation).

NOTE on WSDL/Policy examples: Patterns of WSDL instances and reference policies for classes of OSCI based scenarios will be developed in a distinct project and be made available in step by step in 2009 as addendum to this document.

Technical NOTE for policy instances: All policies defined for an endpoint MUST carry an Id-Attribute for the outer element **`/wsp:Policy/@wsu:Id`** to be referenceable for policy attachment and metadata exchange purposes.

10.1.1 WSDL and Policies for MEP synchronous point-to-point

For this communication scenario, description of endpoint requirements and abilities SHOULD be outlined in one WSDL containing all services and ports with their respective policies available here. Following general reqirements MUST be considerered when designing WSDL instances:

[21] This work is done in the context of the OSCI Profiling project and will be published as an addendum to this specification. Results are planned to be brought to the appropriate OASIS standardization body.

R1200 - A **/wsdl11:port** MUST always contain an entry **/wsa:EndpointReference** with the …**/wsa:Address** element as well as …**/wsa:ReferenceParameters** outling the URI of the …**/osci:TypeOfBusinessScenario** served by this port[22]. Each specific **/osci:TypeOfBusinessScenario** itself correlates to a concrete Content Data message structure given by the **/wsdl11:port** reference chain to a **/wsdl11:binding** and **/wsdl11:portType** entry in this WSDL instance.

10.1.2 WSDL and Policies for asynchronous MEPs via Message Boxes

These MEPs at least have two endpoints in view a message is targeted to:

- Initially, a Source Application has to build up the SOAP body content according to a concrete schema bound to the actuall underlying **/osci:TypeOfBusinessScenario.** In addition, security requirements bound to the Recipient apply like End-to-end encryption and digital signatures to be applied to Content Data, which SHOULD be expressed by according WS Security Policy expressions.
- For transport to the Recipients MsgBox instance, the WSDL and policies of this target node apply. For every **/osci:TypeOfBusinessScenario** accepted here, the body structure is of type **xenc:EncryptedData**. The WS Security Policy if effect here MUST NOT lead to initiate body decrption processing, as the therefore needed private encryption key is only known to the Recipient node.

As of today known WS-Framework implementations, WS Security Policies attached in the WSDL of the node a message is targeted to are completely in effect at the targeted node; it is not possible to bind them e.g. to a specific **s12:role** without in-deepth change of processing logic of standard WS-Framework implementations.

To solve this problem, for this version of the OSCI Transport specification following recommendation applies[23]:

- The MsgBox node exposes the WSDL and policies according his needs on opaque body, transport security and authentication/authorization per accepted **/osci:TypeOfBusinessScenario.**
- WSDL and policies in effect for the Recipient node are referenced or contained in the **/wsa:EndpointReference/wsa:Metadata** element as decribed in chapter [6.1.1], bound to the **/wdsl11:port** policy attachment point.

10.2 OSCI specific Characteristics of Endpoints

To enable OSCI endpoints to describe their requirements and capabilities, this specification defines OSCI policy assertions that leverage the WS-Policy framework. In general, it is RECOMMENDED to attach the policy assertions defined here to a to a port [WSDL11] respective endpoint [WSDL20] policy subject.

10.2.1 Certificates used for Signatures and Encryption

For OSCI based message exchange, X.509v3-Certificates MUST be used for following purposes:

- Encryption to be processed on Initiator side
  - End-to-end encryption of Content Data targeted from a Source Application to a Target Application

[22] following chapter [6.1.1], use of WS-Addressing in OSCI

[23] A WSDL/Policies template for this MEP as well as MsgBox access thru the recipient will be made available as addendum immediately after publishing this specification

- Transport encryption, in cases where asymmetric encryption is required by a specifics application scenario – in general expressed by an adequate security policy

- Certificates used for signatures at Recipient side (respective his MsgBox service); an Initiator MAY – in cases of doubt - cross-check whether received signatures are generated with the certificates exposed in this endpoint policy (detection of possible man-in-the-middle attacks):
  - Signature application for OSCI receipts and possible other message parts – in cases where the signature must be useable for long term provableness
  - If offered: Generation of cryptographic time stamps.

Additional application purposes MAY be defined and supported by dedicated implementations.

Syntax for the OSCI policy containing assertions for X.509v3-Certificates usages:

```
<wsp:Policy wsu:Id="xs:ID">
  <osci:X509CertificateAssertion>
    <wsp:ALL>
      <wsse:SecurityTokenReference wsu:Id="xs:ID" ?
         Usage=
  "http://www.osci.eu/2008/05/common/names/TokenUsage/e2eContentEncryption"
  |
  "http://www.osci.eu/2008/05/common/names/TokenUsage/TransportEncryption"
  |
  "http://www.osci.eu/2008/05/common/names/TokenUsage/ReceiptSigning"
  |
  "http://www.osci.eu/2008/05/common/names/TokenUsage/TSPSigning" *
        osci:Role=
          "http://www.osci.eu/ws/2008/05/transport/role/Recipient" |
          "http://www.osci.eu/ws/2008/05/transport/role/MsgBox" |
          "http://www.w3.org/2003/05/soap-envelope/role/ultimateReceiver" * >

     ( <wsse:Embedded ValueType="xs:anyURI" ? >
         <wsse:BinarySecurityToken  wsu:Id="xs:ID" ?
             ValueType=
               "http://docs.oasis-open.org/wss/2004/01/
                  oasis-200401-wss-x509-token-profile-1.0#X509v3"
             EncodingType=
                "http://docs.oasis-open.org/wss/2004/01/
                 oasis-200401-wss-soapmessage-security-1.0#Base64Binary" >
          xs:base64Binary
         </wsse:BinarySecurityToken>
      </wsse:Embedded> )
         |
     ( <wsse:Reference URI="xs:anyUri"
             ValueType=
               "http://docs.oasis-open.org/wss/2004/01/
                  oasis-200401-wss-x509-token-profile-1.0#X509v3" /> )
         |
     ( <wsse:KeyIdentifier wsu:Id="xs:ID" ?
            ValueType=
                "http://docs.oasis-open.org/wss/
                   oasis-wss-soap-message-security-1.1#ThumbprintSHA1"
            EncodingType=
                "http://docs.oasis-open.org/wss/2004/01/
                   oasis-200401-wss-soapmessage-security-1.0#Base64Binary">
            xs:base64Binary
      </wsse:KeyIdentifier> )

     </wsse:SecurityTokenReference
    </wsp:ALL>
  <osci:X509CertificateAssertion>
<wsp:Policy>
```

Description of elements and attributes in the schema overview above:

`/wsp:Policy`

The whole assertion MUST be embedded in a policy block according to WS Policy.

/wsp:Policy/@wsu:Id

To be referenceable, the policy MUST carry an attribute of type **xs:ID**.

/wsp:Policy/osci:X509CertificateAssertion

The policy block containing all assertions.

/wsp:Policy/osci:X509CertificateAssertion/wsp:ALL

Following the semantics of WS Policy Framework [WSPF], all behaviours represented by the assertions embedded in this block are required/valid.

/wsp:Policy/osci:X509CertificateAssertion/wsp:ALL/wsse:SecurityTokenReference

This element defined in WS Security [WSS] MUST be used as container for a single X.509v3-Certificate (or a reference to it) and its attributes.

As all single certificate details are contained in this block, for brevity full path qualification **/wsp:Policy/osci:X509CertificateAssertion/wsp:ALL/wsse:SecurityTokenReference** is symbolized by **[SingleToken]** in the following descriptions.

[SingleToken]/@wsu:id

A certificate contained/described in this policy MUST be uniquely referenceable – i.e., from other policies describing the same endpoint. This attribute of type **xs:ID** MUST carry an appropriate unique value.

[SingleToken]/@Usage

This attribute defines the purposes a certificate is used for, at least one of the URIs outlined above MUST be supplied as value in this attribute of type list of **xs:anyURI**.

Predefined usage semantics are:

Usage for	URI
End-to-end encryption of Content Data	**http://www.osci.eu/2008/05/common/names/TokenUsage/e2eContentEncryption**
Asymmetric transport encryption	**http://www.osci.eu/2008/05/common/names/TokenUsage/TransportEncryption**
Signature of OSCI receipts; also applicable for signatures of other message parts	**http://www.osci.eu/2008/05/common/names/TokenUsage/ReceiptSigning**
Generation of cryptographic time stamps	**http://www.osci.eu/2008/05/common/names/TokenUsage/TSPSigning**

Table 8: OSCI X.509-Token usages

[SingleToken]/@osci:Role

This attribute defines logical roles a certificate is assigned to, at one of the URIs outlined above MUST be supplied value in this attribute of type list of **xs:anyURI**. Regularly, a single certificate SHOULD NOT be assigned to more the one role; as constellations are imaginable, where logical roles are pooled – like for a Recipient and Ultimate Recipient which are using the same signature certificate - is these cases more then one role assignment MAY be used.

For example, this role attribute allows Initiators to control, whether a receipt is signed with the right certificate used by the septic receipt issuer role outlined in the receipt.

Predefined logical roles are:

Usage for	URI
OSCI Recipient – i.e. using this certificate for signing DeliveryReceipts in synchronous case or as transport encryption certificate	**http://www.osci.eu/ws/2008/05/transport/role/Recipient**
Ultimate receiver in the sense of [SOAP12]; i.e. an Ultimate Recipient using this certificate for end-to-end encryption or ReceptionReceipt signing	**http://www.w3.org/2003/05/soap-envelope/role/ultimateReceiver**
MsgBox service node; i.e. may have his own transport encryption certificate (as MUST be used for "one time tokens")	**http://www.osci.eu/ws/2008/05 /common/names/role/MsgBox**

Table 9: SOAP/OSCI roles assigned to token usages

R1200 - Inside a [SingleToken], the certificate itself may be embedded, referenced or identified by a thumbprint. Other choices foreseen by WS-Security for **/wsse:SecurityTokenReference** MUST NOT be used.

Choice for embedded tokens

[SingleToken]/wsse:Embedded

This choice MUST be taken for embedding X.509v3-Certificates. It is strongly RECOMMENDED to use this choice for certificates to be used for encryption purposes, as an Initiator and STS may need the respective public key for encryption. Referencing those certificates could cause additional to network connection needs.

[SingleToken]/wsse:Embedded/@ValueType

This element MAY carry this attribute of type xs:anyURI. It is not used in the context of this policy.

[SingleToken]/wsse:Embedded/wsse:BinarySecurityToken

Generic container to carry security tokens in binary format; MUST contain the X.509v3-Certificate in base64Binary format.

[SingleToken]/wsse:Embedded/wsse:BinarySecurityToken/@wsu:Id

This attribute of type **xs:ID** is optional. It is not used in the context of this policy.

[SingleToken]/wsse:Embedded/wsse:BinarySecurityToken/@ValueType

As only X.509v3-Certificates are described/contained here, the URI outlined above MUST be supplied as value in this attribute of type of **xs:anyURI**.

[SingleToken]/wsse:Embedded/wsse:BinarySecurityToken/@EncodingType

Hence X.509v3-Certificates MUST be encoded in base64Binary format here, the URI outlined above MUST be supplied as value in this attribute of type of **xs:anyURI**.

Choice for directly referencing tokens

[SingleToken]/wsse:Reference

This choice MUST be taken if referencing X.509v3-Certificates stored otherwise.

[SingleToken]/wsse:Reference/@URI

This attribute of type **xs:anyURI** MUST identify a X.509v3-Certificate. If a fragment is specified, then it indicates the local ID of the security token being referenced. The URI MUST NOT identify a **/wsse:SecurityTokenReference** element, a **/wsse:Embedded** element, a **/wsse:Reference** element, or a **/wsse:KeyIdentifier** element.

[SingleToken]/wsse:Reference/@ValueType

As only X.509v3-Certificates are described/contained here, the URI outlined above MUST be supplied as value in this attribute of type of **xs:anyURI**.

Choice for referencing tokens by thumbprint

This choice SHOULD NOT be used for certificates to be used for encryption purposes, as this may burden Initiator and STS to locate the needed public key for encryption.

[SingleToken]/wsse:KeyIdentifier

R1210: This choice MUST be taken if referencing X.509v3-Certificates by thumbprint. Other choices foreseen by WS-Security for **/wsse:KeyIdentifier** MUST NOT be used.

[SingleToken]/wsse:KeyIdentifier/@wsu:Id

This attribute of type **xs:ID** is optional. It is not used in the context of this policy.

[SingleToken]/wsse:KeyIdentifier/@ValueType

As only thumbprints are allowed for referencing here, the URI outlined above MUST be supplied as value in this attribute of type of **xs:anyURI**.

[SingleToken]/wsse:KeyIdentifier/@EncodingType

Hence thumbprints MUST be encoded in base64Binary format here, the URI outlined above MUST be supplied as value in this attribute of type of **xs:anyURI**.

NOTE on usage of alternate certificates for the same purpose and role:

If more than one certificate may be used for a combination of **[SingleToken]/@osci:Role** and **[SingleToken]/@wsse:Usage,** these policy elements **/wsse:SecurityTokenReference** MUST be grouped in a /**wsp:ExactlyOne** container to express that only one of the alternatives may be chosen.

10.2.2 Endpoint Services and Limitations

OSCI Recipients respective MsgBox services MAY offer/expose following services and limits:

- Qualified timestamp application for signatures; this service is requestable by an Initiator for receipts;
- Message lifetime control; this service interprets the /**osci:MsgTimeStamps/osci:ObsoleteAfter** SOAP header element probably set by an Initiator. This marker only makes sense in asynchronous MEPs, hence the processing policy assigned to is only of interest for MsgBox instances;
- Maximum accepted message size and acceptance frequency per hour.

Syntax for OSCI endpoint services policy assertions:

```
<wsp:Policy wsu:Id="xs:ID">

 <osci:QualTSPAssertion PolicyRef="xs:anyURI"? > ?

 <osci:ObsoleteAfterAssertion PolicyRef="xs:anyURI" ? > ?
  <osci:MsgRetainDays>
   xs:positiveInteger
  </osci:MsgRetainDays> ?
```

```
    <osci:WarningMsgBeforeObsolete>
      xs:nonNegativeInteger
    </osci:WarningMsgBeforeObsolete> ?
  </osci:ObsoleteAfterAssertion> ?

  <osci:MsgLimitsAssertion>
     <osci:MaxSize>
       xs:positiveInteger
     </osci:MaxSize> ?
     <osci:MaxPerHour>
       xs:positiveInteger
     </osci:MaxPerHour> ?
  </osci:MsgLimitsAssertion> ?

<wsp:Policy>
```

Description of elements and attributes in the schema overview above:

/wsp:Policy

The whole assertion MUST be embedded in a policy block according to WS Policy.

/wsp:Policy/@wsu:Id

To be referenceable, the policy MUST carry an attribute of type **xs:ID**.

/wsp:Policy/osci:QualTSPAssertion ?

The presence of this element signals the availability of a qualified timestamp service.

/wsp:Policy/osci:QualTSPAssertion/@PolicyRef ?

This optional attribute of type **xs:anyURI** SHOULD be provided and carry a link to i.e. human readable policies describing terms and conditions under which this service is made available.

/wsp:Policy/osci:ObsoleteAfterAssertion ?

The presence of this element signals the fact this endpoint will care about a SOAP header entry /**osci:MsgTimeStamps/osci:ObsoleteAfter.**

/wsp:Policy/osci:ObsoleteAfterAssertion/@PolicyRef ?

This optional attribute of type **xs:anyURI** MAY be provided and carry a link to i.e. human readable policies describing terms and conditions about deletion of messages marked to be obsolete meanwhile.

/wsp:Policy/osci:ObsoleteAfterAssertion/MsgRetainDays ?

This optional element of type **xs:positiveInteger** SHOULD be provided to expose the number of days a message still is hold available after the date provided by the .../**osci:ObsoleteAfter** entry.

/wsp:Policy/osci:ObsoleteAfterAssertion/WarningBeforeObsolete ?

This optional element of type **xs:nonNegativeInteger** SHOULD be provided to expose the number of days a warning is generated before the date provided by the .../**osci:ObsoleteAfter** entry. Thus, an escalation procedure could be triggered for messages seen to be of high importance. How this warning is generated and delivered is a matter of implementation of this service and SHOULD be described in the terms and conditions policy.[24]

/wsp:Policy/osci:MsgLimitsAssertion ?

[24] This warning could i.e. be delivered in the body of an osci:Request to the Initiator alike the FetchedNotification message.

The presence of this element signals the fact this endpoint has restrictions for incoming messages.

/wsp:Policy/osci: MsgLimitsAssertion/MaxSize ?

This optional element of type **xs:positiveInteger** outlines the maximum size in kilobytes for incoming messages this endpoint accepts.

If an incoming message exceeds this limit, it MUST be withdrawn and a fault MUST be returned to the targeting node:

Fault 13: MsgSizeLimitExceeded
[Code] Sender
[Subcode] MsgSizeLimitExceeded
[Reason] Message size exceeds policy

/wsp:Policy/osci: MsgLimitsAssertion/MaxPerHour ?

This optional element of type **xs:positiveInteger** outline the maximum amount in of messages accepted per hour from the same originating node[25].

If an incoming messages originated from the same targeting node exceed this limit, the message MUST be withdrawn and a fault MUST be returned to the targeting node:

Fault 14: MsgFrequencyLimitExceeded
[Code] Sender
[Subcode] MsgFrequencyLimitExceeded
[Reason] Message frequency per hour exceeds policy

10.3 WS Addressing Metadata and WS MakeConnection

Hence the use of WS-Addressing is mandatory for OSCI, an endpoint policy MUST contain WS-Addressing properties described here in terms of WS-Addressing Metadata [WSAM] .

Following policy assertions MUST be bound to the **wsld11:port** (WSDL 2.0: endpoints) or **wsdl11:binding** endpoint policy subjects which accept messages of type osci:Request; WS MakeConnection is not supported in this case:

```
<wsp:Policy wsu:Id="xs:ID" ?>
    <wsam:Addressing>
      <wsp:Policy/> ?
    </wsam:Addressing>
</wsp:Policy>
```

This policy ascertains the use of WS-Addressing and that the endpoint requires request messages to use response endpoint EPRs that contain something other than the anonymous URI as the value in the SOAP header element **/wsa:ReplyTo/wsa:Address.**

```
<wsp:Policy wsu:Id="xs:ID" ?>
    <wsmc:MCSupported/>
</wsp:Policy> ?
```

This policy assertion MUST only be used, if WS MakeConnection is supported by this endpoint (see chapter [6.2]). In this case, the value of **/wsa:ReplyTo/wsa:Address** MUST be the WS-MC anonymous URI template

[25] No further details defined here, it is left to implementations how to define appropriate count starting and reset points

http://docs.oasis-open.org/ws-rx/wsmc/200702/anonymous?id={unique-String}.

Following policy assertions MUST be bound **to wsdl11:ports** (WSDL 2.0: endpoints) or **wsdl11:binding** policy subjects accepting messages for MsgBox access - these are the message of type MsgBoxFetchRequest, MsgBoxStatusListRequest, MsgBoxGetNextRequest and MsgBoxCloseRequest:

```
<wsp:Policy wsu:Id="xs:ID" ?>
  <wsam:Addressing>
     <wsp:Policy>
       <wsam:AnonymousResponses/>
     <wsp:Policy>
  </wsam:Addressing>
</wsp:Policy>
```

This policy ascertains the use of WS-Addressing and that the endpoint requires request messages to use response endpoint EPRs that carry an URI value of

"http://www.w3.org/2005/08/addressing/anonymous"

in the SOAP header element **/wsa:ReplyTo/wsa:Address**.

10.4 WS Reliable Messaging Policy Assertions

Support of WS Reliable Messaging is an optional feature of conformant implementations. If supported, adequate policy assertions SHOULD be used to ascertain the details of reliable messaging exchange. We refer to the specification WS Reliable Messaging Policy Assertions Version 1.1 [WSRMP] in this point with no further profiling.

10.5 MTOM Policy Assertion

The SOAP Message Transmission Optimization Mechanism [MTOM] MUST be supported by conformant implementations. The MTOM policy assertion MUST be attached to either a **wsdl11:binding** or **wsdl11:port** endpoint policy subject. It is expressed as

```
<wsp:Policy wsu:Id="xs:ID" ?>
    <wspmtom:OptimizedMimeSerialization/>
</wsp:Policy> ?
```

We refer to the specification draft [MTOMP].

10.6 WS Security Profile and Policy Assertions

10.6.1 Endpoint Policy Subject Assertions

10.6.1.1 Symmetric Binding

The symmetric binding assertion defines details of message protection by means of WS-Security [WSS]. In both directions from the Initiator to the Recipient or his MsgBox instance and backwards the same security tokens are used for transport level encryption and signature.

According to [WSSP], this assertion SHOULD apply to the endpoint policy subject **wsdl11:binding**; it MAY apply to operation policy subject **wsdl11:binding/wsdl11:operation**.

Requirements outlined in this document for message security lead to following restrictions of overall options defined by WS Security Policy (see [WSSP], chapter 7.4).

As described in chapter [7.5, R0600], SAML Token issued by STS instances MUST be used, which here leads to:

R1230 - This profiling restricts to the usage of **wssp:ProctectionToken**; distinct **wssp:EncryptionToken** and **wssp:SignatureToken** MUST NOT be used.

10.6.1.2 Asymmetric Binding

For the asymmetric binding, public keys of X.509v3 certificates are used as security tokens. The support of this binding is OPTIONAL; it MUST be used in case of anonymous access is supported as described in chapter [6.2].

According to [WSSP], this assertion SHOULD apply to the endpoint policy subject **`wsdl11:binding`**; it MAY apply to operation policy subject **`wsdl11:binding/wsdl11:operation`**.

Used certificates MUST have the according key usage set; R0610 and R0620 (see chapter [7.4]) apply here and in addition:

R1240 - The node a message is targeted to MUST verify the validity of certificates used for encryption; in case a value other than valid at time of usage is stated, the message MUST be discarded and a fault MUST be generated.

Fault 15: **EncryptionCertNotValid**	
[Code]	Sender
[Subcode]	EncryptionCertNotValid
[Reason]	Encryption certificate not stated to be valid

More information about the certificate validation results SHOULD be provided in the fault [Details] property in this case. It is strongly RECOMMENDED to log such faults to be able to detect possible security violation attacks.

In the context with certificates used by a Recipient oder his MsgBox node as described in the chapter [10.2.1], the assertions **`/wssp:RecipientEncryptionToken`** and **`/wssp:RecipientSignatureToken`** SHOULD point to the according certificate entries in in the Recipients metadata file.

10.6.1.3 Transport Binding

The transport binding MAY be used in scenarios in which message protection and security correlation is provided by means other than WS-Security. We restrict to HTTPS here:

R1250 - HTTPS MUST be used, if message protection is provided by the underlying transport protocal.

This assertion MUST apply to the endpoint policy subject **`wsdl11:binding`**.

10.6.2 Message Policy Subject Assertions

[WSSP] offers policy statements for directions, which message parts must be present and which message parts have to be signed and encrypted. For the here presented profiling, assertions on the SOAP header and body block level are REQUIRED, assertions on element level according to [WSSP] MAY be used in addition.

Following outlines only show the syntax of these assertions; following requirement applies:

R1260 - Concrete instances MUST enumerate the header and body blocks marked as mandatory for presence, to be signed and/or encrypted according to definitions made per message type in chapter [9, Constituents of OSCI Message Types].

Required message parts policy assertion:

```
<wsp:Policy>
  <wsp:ALL>
    <wssp:RequiredParts xmlns:wssp="..." ... >
      <wssp:Header Name="xs:NCName"? Namespace="xs:anyURI" ... /> +
    </wssp:RequiredParts>
  </wsp:ALL>
</wsp:Policy>
```

Signed message parts policy assertion:

```
<wsp:Policy>
  <wsp:ALL>
     <wssp:SignedParts xmlns:wssp="..." ... >
       <wssp:Body />
       <wssp:Header Name="xs:NCName"? Namespace="xs:anyURI" ... /> +
     </wssp:SignedParts>
  </wsp:ALL>
</wsp:Policy>
```

NOTE: According to R1230, the SOAP body block always MUST be included in the transport signature to ensure integrity of coherence with the message header block parts.

Encrypted message parts policy assertion:

```
<wsp:Policy>
  <wsp:ALL>
     <wssp:EncryptedParts xmlns:wssp="..." ... >
       <wssp:Body /> ?
       <wssp:Header Name="xs:NCName"? Namespace="xs:anyURI" ... /> *
     </wssp:EnryptedParts>
  </wsp:ALL>
</wsp:Policy>
```

If potentially unsecured network connections are used for message exchange, following requirement applies:

R1270 - If the Content Data carried in the SOAP body is not encrypted end-to-end, the body block MUST be transport encrypted.

To include the required SOAP header blocks of the different OSCI message types, following requirement applies:

R1280 - These policy assertions MUST be bound to the message policy subject:

wsdl11:binding/wsdl11:operation/wsdl11:input

respective

wsdl11:binding/wsdl11:operation/wsdl11:output

10.6.3 Algorithm Suite Assertions

In the chapters [7.2.1 and 7.3.2], restrictions are defined to suitable crytographic algorithms, which leads to following restrictions[26]:

R1290 - For the symmetric case, following restriction applies for the algorithm suite assertion:

```
<wsp:Policy>
  <wssp:AlgorithmSuite>
     <wsp:Policy>
       ( <wssp:Basic256Sha256 ... /> |
         <wssp:Basic192Sha256 ... /> |
         <wssp:Basic128Sha256 ... /> |
       <wssp:TripleDesSha256 ... /> )
     </wsp:Policy>
   </wssp:AlgorithmSuite>
</wsp:Policy>
```

R1300 - For the asymmetric case, following restriction applies for the algorithm suite assertion:

```
<wsp:Policy>
  <wssp:AlgorithmSuite>
```

[26] As of today, there are not yet algorrihm identifier assertions defined for SHA512 and RIPEMD160. As these are recommended algorithms, this will be aligned with the reposible OASIS TC and completed as soon as possible by corrigenda for this document.

```
    <wsp:Policy>
      ( <wssp:Basic256Sha256Rsa15 ... /> |
        <wssp:Basic192Sha256Rsa15 ... /> |
        <wssp:Basic128Sha256Rsa15 ... /> |
        <wssp:TripleDesSha256Rsa15 ... /> )
    </wsp:Policy>
  </wssp:AlgorithmSuite>
</wsp:Policy>
```

The scope of these assertions is defined by its containing assertion.

R1310 - Algorithm suite assertions MUST at least be included in assertions bound to the the endpoint poliy subject **`wsdl11:binding.`** In addition, variations MAY be bound to subordinary policy subjects to express specific requirements.

11 Applying End-to-end Encryption and Digital Signatures on Content Data

Predominant for OSCI is exchange of data in an authentic, confidential manner with support for legal binding. Hence, functionalities are needed for Content Data end-to-end encryption and decryption, application of digital signatures to Content Data and signature validation.

To ensure interoperability and conformance with the EC-Directive on Digital Signatures as well the German Signature Law and -Ordinance and underlying technical specifications, these optional functionalities – if provided – MUST be realized conformant to the "Common PKI Specifications for Interoperable Applications, Part 7: Signature API" [COMPKI]. This specification is a subset of the "eCard-API Framework" [eCardAPI], based on standards worked out by the OASIS Digital Signature Services Technical Committee [DSS].

The Common PKI Signature API defines an XML interface for – among others – following functions:

- SignRequest
- VerifyRequest
- EncryptRequest
- DecryptRequest.

API bindings are defined for C and Java; on base of the XML definitions the defined functions could also be realized as services provided by an OSCI Gateway implementation.

To use the OSCI-feature of certificate validation on the message route, messages producing instances SHOULD supply certificates used for cryptographical operations on Content Data level in a structure described as "X.509-Token Container" in chapter [8.4.1]. This container must be carried in a message as custom SOAP header block.

On the message consuming side, the resulting custom SOAP headers **`/xkms:ValidateResponse`** SHOULD be used to simplify signature verification, as the burden of connecting to CAs is delegated to specialized nodes on the message route. See chapter [8.4] for details.

12 Indices

12.1 Tables

12.2 Pictures

12.3 OSCI specific faults

12.4 Listings

13 References

13.1 Normative

[AlgCat] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, 17. November 2008, http://www.bundesnetzagentur.de/media/archive/14953.pdf

[COMPKI] Common PKI Specifications for interoperable Applications, Version 2.0, 20 January 2009; http://www.common-pki.org/uploads/media/Common-PKI_v2.0.pdf

[eCardAPI] Das eCard-API-Framework (BSI TR-03112). Version 1.0, Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik), March 2008, http://www.bsi.de/literat/tr/tr03112/index.htm

[DSS] Digital Signature Service Core - Protocols, Elements, and Bindings Version 1.0, OASIS Standard, 11 April 2007; http://www.oasis-open.org/specs/index.php#dssv1.0

[MTOM] SOAP Message Transmission Optimization Mechanism, W3C Recommendation 25 January 2005, http://www.w3.org/TR/soap12-mtom/

[MTOMP] MTOM Policy Assertion 1.1, W3C Working Draft 18 September 2007, http://www.w3.org/TR/soap12-mtom-policy/

[PKCS#1] B. Kaliski, J. Staddon: PKCS #1: RSA Cryptography Specifications – Version 2.0, IETF RFC 2437, The Internet Society October 1998, http://www.ietf.org/rfc/rfc2437.txt

[RFC2119] S. Bradner, **Key words for use in RFCs to Indicate Requirement Levels,** RFC 2119, Harvard University, March 1997, http://www.ietf.org/rfc/rfc2119.txt

[RFC2396] T. Berners-Lee, R. Fielding, U.C. Irvine, L. Masiner, Uniform Ressource Identifiers (URI): Generic Syntax, RFC 2396, The Internet Society 1998; http://www.ietf.org/rfc/rfc2396.txt

[RFC3161] D. Pinkas, R. Zuccerato, Time-Stamp Protocol (TSP), IETF RFC 1661, http://www.ietf.org/rfc/rfc3161.txt

[RFC4122] A Universally Unique Identifier (UUID) URN Namespace, The Internet Engeneering Task Force July 2005, http://www.ietf.org/rfc/rfc4122.txt

[SAFE] S.A.F.E. (Secure Access to Federated e-Justice/e-Government) / D.I.M. (Distributed Identity Management), Unterarbeitsgruppe SAFE der BLK Arbeitsgruppe ITStandards in der Justiz, April 2008, http://www.justiz.de/ERV/Grob-_und_Feinkonzept/index.php

[SAMLAC] Auhtentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 March 2005, http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf

[SAML2] Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 March 2005; http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[SOAP12] SOAP Version 1.2 Part 1: Messaging Framework (Second Edition), W3C Recommendation 27 April 2007, http://www.w3.org/TR/soap12-part1/

[WSA] Web Services Addressing 1.0 - Core, W3C Recommendation 9 May 2006, http://www.w3.org/TR/2006/REC-ws-addr-core-20060509/

[WSAM] Web Services Addressing 1.0 - Metadata, W3C Proposed Recommendation 31 July 2007, http://www.w3.org/TR/ws-addr-metadata/

[WSASOAP] Web Services Addressing 1.0 – SOAP Binding, W3C Recommendation 9 May 2006, http://www.w3.org/TR/2006/REC-ws-addr-soap-20060509/

[WSAW] Web Services Addressing 1.0 – WSDL Binding, W3C Candidate Recommendation 29 May 2006, http://www.w3.org/TR/ws-addr-wsdl/

[WSDL20] Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language, W3C Recommendation 26 June 2007, http://www.w3.org/TR/wsdl20/

[WSDL11] Web Services Description Language (WSDL) 1.1: W3C Note 15 March 2001, http://www.w3.org/TR/2001/NOTE-wsdl-20010315

[WSDLA] Web Services Description Language (WSDL) Version 2.0 Part 2: Adjuncts, W3C Recommendation 26 June 2007, http://www.w3.org/TR/2007/REC-wsdl20-adjuncts-20070626/

[WSF] Web Services Federation Language (WS-Federation), Version 1.1, December 2006, http://specs.xmlsoap.org/ws/2006/12/federation/ws-federation.pdf

[WSI-Basic] WS-I Basic Profile 2.0, Working Group Draft, 2007-10-25, WEB SERVICES INTEROPERABILITY ORGANIZATION, http://www.ws-i.org/Profiles/BasicProfile-2_0(WGD).html

[WSI-BP11] WS-I Basic Profile 1.1, Final Material, 2006-04-10, WEB SERVICES INTEROPERABILITY ORGANIZATION, http://www.ws-i.org/Profiles/BasicProfile-1.1.html

[WSI-BSP11] WS-I Basiy Security Profile Version 1.1, Wokring Group Approval Draft, 2007-02-20, WEB SERVICES INTEROPERABILITY ORGANIZATION, http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html

[WSMC] Web Services Make Connection (WS MakeConnection), Version 1.0, OASIS Standard, 14 June 2007, http://docs.oasis-open.org/ws-rx/wsmc/200702/wsmc-1.0-spec-os-01.pdf

[WSPA] Web Services Policy 1.5 - Attachment, W3C Recommendation, 4 September 2007; http://www.w3.org/TR/2007/REC-ws-policy-attach-20070904/

[WSPF] Web Services Policy 1.5 - Framework, W3C Recommendation, 4 September 2007; http://www.w3.org/TR/2007/REC-ws-policy-20070904/

[WSRM] Web Services Reliable Messaging (WS-ReliableMessaging) Version 1.1, OASIS Standard Specification incorporating approved Errata, 07 January 2008, http://docs.oasis-open.org/ws-rx/wsrm/200702/wsrm-1.1-spec-os-01-e1.pdf

[WSRMP] Web Services Reliable Messaging Policy Assertion (WS-RM Policy) Version 1.1 OASIS Standard Specification incorporating approved Errata, 07 January 2008, http://docs.oasis-open.org/ws-rx/wsrmp/200702/wsrmp-1.1-spec-os-01-e1.pdf

[WSS] Web Services Security: SOAP Message Security 1.1, OASIS Standard Specification, 1 February 2006, http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf

[WSS10] Web Services Security: SOAP Message Security 1.0 (WS-Security 200), OASIS Standard 200401, March 2004, http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf

[WSSC] Web Services Secure Conversation 1.3, OASIS Standard, 1 March 2007, http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512/ws-secureconversation-1.3-os.pdf

[WSSP] WS-SecurityPolicy 1.2, OASIS Standard 1 July 2007, http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-1.2-spec-os.pdf

[WSSKERB] Web Services Security Kerberos Token Profile 1.1, OASIS Standard Specification, incorporating Approved Errata, 1 November 2006, http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-errata-os-KerberosTokenProfile.pdf

[WSSSAML] Web Services Security SAML Token Profile 1.1, OASIS Standard Specification incorporating Approved Errata, 1 November 2006, http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-errata-os-SAMLTokenProfile.pdf

[WSSUSER] Web Services Security Username Token Profile 1.1, OASIS Standard Specification, 1 February 2006, http://www.oasis-open.org/committees/download.php/16782/wss-v1.1-spec-os-UsernameTokenProfile.pdf

[WSSX509] Web Services Security X.509 Certificate Token Profile 1.1, OASIS Standard Specification, incorporating Approved Errata, 1 November 2006, http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-errata-os-x509TokenProfile.pdf

[WST] WS-Trust 1.3, OASIS Standard, 19 March 2007, http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf

[XAdES] European Telecommunications Standards Institute. ETSI TS 101 903: XML Advanced Electronic Signatures, V1.3.2 2006-03; http://webapp.etsi.org/action/PU/20060307/ts_101903v010302p.pdf .

[XENC] World Wide Web Consortium. XML Encryption Syntax and Processing, W3C Recommendation, 10.12.2002; http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/

[XKMS] XML Key Management Specification (XKMS 2.0) v2, W3C Recommendation, 28 June 2005, http://www.w3.org/TR/2005/REC-xkms2-20050628/

[XKMSEU] PEPPOL XKMS v2 Interface Specification, Version 1.2, PEPPOL WP1 2009-04-30, copy at http://www.osci.eu/transport/osci2/specification/PEPPOL_D1.1_v1.2_XKMS InterfaceSpecification

[XMLDSIG] World Wide Web Consortium. XML-Signature Syntax and Processing (Second Edition), W3C Recommendation, 10 June 2008; http://www.w3.org/TR/xmldsig-core/

[XMLSchema] World Wide Web Consortium. XML Schema, Parts 0, 1, and 2 (Second Edition). W3C Recommendation, 28 October 2004; http://www.w3.org/TR/xmlschema-0/, http://www.w3.org/TR/xmlschema-1/, and http://www.w3.org/TR/xmlschema-2/

[XML 1.0] World Wide Web Consortium. Extensible Markup Language (XML) 1.0 (Fourth Edition), T. Bray, J. Paoli, C. M. Sperberg-McQueen, and E. Maler, Editors. 10

February 1998, revised 16 August 2006; http://www.w3.org/TR/2006/REC-xml-20060816/

[XPATH 1.0] W3C Recommendation, "XML Path Language (XPath) Version 1.0," 16 November 1999; http://www.w3.org/TR/xpath

13.2 Informative

[WSFED] Web Services Federation Language (WS-Federation), Version 1.2, latest TC/Editor Draft see: http://www.oasis-open.org/committees/documents.php?wg_abbrev=wsfed

[WSMEX] Web Services Metadata Exchange, Version 1.1, W3C Member Submission 13 August 2008, http://www.w3.org/Submission/2008/SUBM-WS-MetadataExchange-20080813/

Appendix A. Schema

OSCI Transport 2.0 Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:wsa="http://www.w3.org/2005/08/addressing"
xmlns:osci="http://www.osci.eu/ws/2008/05/transport" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:s12="http://www.w3.org/2003/05/soap-envelope"
xmlns:wsp="http://www.w3.org/ns/ws-policy" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
targetNamespace="http://www.osci.eu/ws/2008/05/transport"
elementFormDefault="qualified" attributeFormDefault="unqualified">
  <!--OSCI Transport Version 2.0 schema - last edited by Joerg Apitzsch/bos as of
2009-06-04-->
  <!--xs:import namespace="http://www.w3.org/2005/08/addressing" schemaLocation="ws-
addr.xsd"/-->
  <xs:import namespace="http://www.w3.org/2005/08/addressing"
schemaLocation="http://www.w3.org/2006/03/addressing/ws-addr.xsd"/>
  <!--xs:import namespace="http://www.w3.org/2000/09/xmldsig#"
schemaLocation="xmldsig-core-schema.xsd"/-->
  <xs:import namespace="http://www.w3.org/2000/09/xmldsig#"
schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd"/>
  <!--xs:import namespace="http://www.w3.org/2003/05/soap-envelope"
schemaLocation="soap-envelope.xsd"/-->
  <xs:import namespace="http://www.w3.org/2003/05/soap-envelope"
schemaLocation="http://www.w3.org/2003/05/soap-envelope/"/>
  <!--xs:import namespace="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" schemaLocation="oasis-200401-wss-wssecurity-utility-
1.0.xsd"/-->
  <xs:import namespace="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" schemaLocation="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"/>
  <!--xs:import namespace="http://www.w3.org/ns/ws-policy" schemaLocation="ws-
policy.xsd"/-->
  <xs:import namespace="http://www.w3.org/ns/ws-policy"
schemaLocation="http://www.w3.org/2007/02/ws-policy.xsd"/>
  <!--xs:import namespace="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" schemaLocation="oasis-200401-wss-wssecurity-secext-
1.0.xsd"/-->
  <xs:import namespace="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" schemaLocation="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"/>
  <!--Roles of OSCI (SOAP) nodes (informational, not referenced by other
definitions) -->
  <xs:simpleType name="Role">
    <xs:list itemType="xs:anyURI"/>
  </xs:simpleType>
  <!--WSA-Extension: BusinessScenarioType-->
  <xs:element name="TypeOfBusinessScenario" type="xs:anyURI"/>
  <!--General header-part of OSCI messages: timestamps-->
  <xs:complexType name="MsgTimeStampsType">
    <xs:sequence>
      <xs:element name="ObsoleteAfter" type="xs:date" minOccurs="0">
        <xs:annotation>
          <xs:documentation>Date, when this message is obsolete; may be set by
Initiator</xs:documentation>
        </xs:annotation>
      </xs:element>
      <xs:element name="Delivery" type="xs:dateTime" minOccurs="0">
        <xs:annotation>
          <xs:documentation>Time of entry in a Recipient MsgBox</xs:documentation>
        </xs:annotation>
      </xs:element>
      <xs:element name="InitialFetch" type="xs:dateTime" minOccurs="0">
```

```
      <xs:annotation>
        <xs:documentation>Time of first comitted fetch from MsgBox by the
Recipient</xs:documentation>
      </xs:annotation>
    </xs:element>
    <xs:element name="Reception" type="xs:dateTime" minOccurs="0">
      <xs:annotation>
        <xs:documentation>Reception Time set by the Recipient</xs:documentation>
      </xs:annotation>
    </xs:element>
  </xs:sequence>
  <xs:attribute ref="wsu:Id" use="required"/>
 </xs:complexType>
 <xs:element name="MsgTimeStamps" type="osci:MsgTimeStampsType"/>
 <!--Types and Elements for MsgBox request/responses-->
 <xs:annotation>
  <xs:documentation>Template for MsgBox-Requests</xs:documentation>
 </xs:annotation>
 <xs:complexType name="MsgBoxRequestType">
  <xs:sequence>
   <xs:element ref="wsa:EndpointReference"/>
   <xs:element ref="osci:MsgSelector" minOccurs="0"/>
  </xs:sequence>
 </xs:complexType>
 <xs:complexType name="MsgBoxResponseType">
  <xs:choice>
   <xs:element name="NoMessageAvailable">
    <xs:complexType>
     <xs:attribute name="reason" type="xs:QName"/>
    </xs:complexType>
   </xs:element>
   <xs:element name="ItemsPending" type="xs:nonNegativeInteger"/>
  </xs:choice>
  <xs:attribute ref="osci:MsgBoxRequestID" use="required"/>
  <xs:attribute ref="wsu:Id"/>
 </xs:complexType>
 <xs:complexType name="MsgAttributeListType">
  <xs:sequence>
   <xs:element ref="wsa:MessageID"/>
   <xs:element ref="wsa:RelatesTo" minOccurs="0" maxOccurs="unbounded"/>
   <xs:element ref="wsa:From"/>
   <xs:element name="BusinessScenarioType" type="xs:QName"/>
   <xs:element ref="wsa:Action"/>
   <xs:element name="MsgSize" type="xs:int"/>
   <!--xs:element ref="osci:MsgTimeStamps"/-->
   <xs:element name="ObsoleteAfterDate" type="xs:date"/>
   <xs:element name="DeliveryTime" type="xs:dateTime"/>
   <xs:element name="InitialFetchedTime" type="xs:dateTime"/>
  </xs:sequence>
 </xs:complexType>
 <xs:attribute name="MsgBoxRequestID" type="xs:anyURI"/>
 <xs:element name="MsgSelector">
  <xs:complexType>
   <xs:sequence minOccurs="0">
    <xs:element ref="wsa:MessageID" minOccurs="0" maxOccurs="unbounded"/>
    <xs:element ref="wsa:RelatesTo" minOccurs="0" maxOccurs="unbounded"/>
    <xs:element name="MsgBoxEntryFrom" type="xs:dateTime" minOccurs="0"/>
    <xs:element name="MsgBoxEntryTo" type="xs:dateTime" minOccurs="0"/>
    <xs:element name="Extension" type="xs:anyType" minOccurs="0"/>
   </xs:sequence>
   <xs:attribute name="newEntry" type="xs:boolean"/>
  </xs:complexType>
 </xs:element>
 <xs:element name="MsgStatusList" type="osci:MsgStatusListType"/>
 <xs:complexType name="MsgStatusListType">
  <xs:sequence>
   <xs:element name="MsgAttributes" type="osci:MsgAttributeListType"
maxOccurs="unbounded"/>
  </xs:sequence>
 </xs:complexType>
```

```
  <xs:element name="MsgBoxFetchRequest" type="osci:MsgBoxRequestType"/>
  <xs:element name="MsgBoxStatusListRequest"
type="osci:MsgBoxStatusListRequestType"/>
  <xs:complexType name="MsgBoxStatusListRequestType">
    <xs:complexContent>
      <xs:extension base="osci:MsgBoxRequestType">
        <xs:attribute name="maxListItems" type="xs:positiveInteger"/>
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>
  <xs:element name="MsgBoxResponse" type="osci:MsgBoxResponseType"/>
  <xs:element name="MsgBoxGetNextRequest" type="osci:MsgBoxGetNextRequestType"/>
  <xs:complexType name="MsgBoxGetNextRequestType">
    <xs:sequence>
      <xs:element ref="wsa:EndpointReference"/>
      <!--
        <xs:element name="LastMsgReceived" type="wsa:AttributedURIType" minOccurs="0"
maxOccurs="unbounded"/>
        -->
    </xs:sequence>
    <xs:attribute ref="osci:MsgBoxRequestID" use="required"/>
  </xs:complexType>
  <xs:element name="MsgBoxClose" type="osci:MsgBoxCloseType"/>
  <xs:complexType name="MsgBoxCloseType">
    <xs:attribute ref="osci:MsgBoxRequestID" use="required"/>
    <!--
      <xs:sequence minOccurs="0">
        <xs:element name="LastMsgReceived" type="wsa:AttributedURIType" minOccurs="0"
maxOccurs="unbounded"/>
      </xs:sequence>
    -->
  </xs:complexType>
  <!--Types and Elements for Receipt- and Notification Handling-->
  <xs:attribute name="qualTSPForReceipt" type="xs:boolean" default="false"/>
  <xs:attribute name="echoRequest" type="xs:boolean" default="false"/>
  <xs:complexType name="ReceiptDemandType">
    <xs:sequence>
      <xs:element ref="wsa:ReplyTo"/>
    </xs:sequence>
    <xs:attribute ref="wsu:Id" use="required"/>
    <xs:attribute ref="s12:role"/>
    <xs:attribute ref="osci:qualTSPForReceipt"/>
    <xs:attribute ref="osci:echoRequest"/>
  </xs:complexType>
  <xs:element name="DeliveryReceiptDemand" type="osci:DeliveryReceiptDemandType"/>
  <xs:element name="ReceptionReceiptDemand" type="osci:ReceptionReceiptDemandType"/>
  <xs:complexType name="ReceiptInfoType">
    <xs:sequence>
      <xs:element ref="wsa:MessageID"/>
      <xs:element ref="osci:MsgTimeStamps"/>
      <xs:element ref="wsa:RelatesTo" minOccurs="0"/>
      <xs:element name="To" type="wsa:EndpointReferenceType"/>
      <xs:element ref="wsa:From" minOccurs="0"/>
      <xs:element ref="wsa:ReplyTo"/>
      <xs:element name="RequestEcho" type="xs:base64Binary" minOccurs="0"/>
    </xs:sequence>
    <xs:attribute ref="wsu:Id" use="required"/>
  </xs:complexType>
  <xs:complexType name="DeliveryReceiptDemandType">
    <xs:complexContent>
      <xs:restriction base="osci:ReceiptDemandType">
        <xs:sequence>
          <xs:element ref="wsa:ReplyTo"/>
        </xs:sequence>
        <xs:attribute ref="s12:role" fixed="http://www.w3.org/2003/05/soap-
envelope/role/next"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>
  <xs:complexType name="ReceptionReceiptDemandType">
```

```
    <xs:complexContent>
      <xs:restriction base="osci:ReceiptDemandType">
        <xs:sequence>
          <xs:element ref="wsa:ReplyTo"/>
        </xs:sequence>
        <xs:attribute ref="s12:role" fixed="http://www.w3.org/2003/05/soap-
envelope/role/ultimateReceiver"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>
  <xs:complexType name="DeliveryReceiptType">
    <xs:sequence>
      <xs:element name="ReceiptInfo">
        <xs:complexType>
          <xs:complexContent>
            <xs:extension base="osci:ReceiptInfoType">
              <xs:attribute name="ReceiptIssuerRole" use="required">
                <xs:simpleType>
                  <xs:restriction base="xs:anyURI">
                    <xs:enumeration
value="http://www.osci.eu/2008/transport/roles/MsgBox"/>
                    <xs:enumeration
value="http://www.osci.eu/2008/transport/roles/Recipient"/>
                  </xs:restriction>
                </xs:simpleType>
              </xs:attribute>
            </xs:extension>
          </xs:complexContent>
        </xs:complexType>
      </xs:element>
      <xs:element ref="ds:Signature"/>
    </xs:sequence>
    <xs:attribute ref="wsu:Id" use="required"/>
  </xs:complexType>
  <xs:element name="DeliveryReceipt" type="osci:DeliveryReceiptType"/>
  <xs:complexType name="ReceptionReceiptType">
    <xs:sequence>
      <xs:element name="ReceiptInfo" type="osci:ReceiptInfoType"/>
      <xs:element ref="ds:Signature"/>
    </xs:sequence>
    <xs:attribute ref="wsu:Id"/>
  </xs:complexType>
  <xs:element name="ReceptionReceipt" type="osci:ReceptionReceiptType"/>
  <xs:complexType name="FetchedNotificationDemandType">
    <xs:sequence>
      <xs:element ref="wsa:ReplyTo"/>
    </xs:sequence>
    <xs:attribute ref="s12:role"
default="http://www.osci.eu/2008/transport/roles/MsgBox"/>
    <xs:attribute ref="wsu:Id"/>
  </xs:complexType>
  <xs:element name="FetchedNotificationDemand"
type="osci:FetchedNotificationDemandType"/>
  <xs:complexType name="FetchedNotificationType">
    <xs:sequence>
      <xs:element name="FetchedTime" type="xs:dateTime"/>
      <xs:element ref="wsa:MessageID"/>
      <xs:element ref="wsa:To"/>
      <xs:element ref="wsa:From"/>
    </xs:sequence>
  </xs:complexType>
  <xs:element name="FetchedNotification" type="osci:FetchedNotificationType"/>
  <!--Extentensions for Key usage context-->
  <xs:complexType name="X509TokenContainerType">
    <xs:sequence maxOccurs="unbounded">
      <xs:element ref="osci:X509TokenInfo"/>
    </xs:sequence>
    <xs:attribute name="validateCompleted" type="xs:boolean" default="false"/>
    <xs:attribute ref="wsu:Id"/>
    <xs:attribute ref="s12:role"/>
```

```
  </xs:complexType>
  <xs:element name="X509TokenContainer" type="osci:X509TokenContainerType"/>
  <xs:element name="X509TokenInfo">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="ds:X509Data"/>
        <xs:element name="TokenApplication" maxOccurs="unbounded">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="TimeInstant" type="xs:dateTime"/>
              <xs:element name="MsgItemRef" type="xs:IDREF" minOccurs="0"/>
            </xs:sequence>
            <xs:attribute name="validateResultRef" type="xs:IDREF"/>
            <xs:attribute name="ocspNoCache" type="xs:boolean"/>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
      <xs:attribute name="validated" type="xs:boolean" default="false"/>
      <xs:attribute name="Id" type="xs:ID" use="required"/>
      <!-- RFC 3280 for KeyUsage with Extentensions Attribute Certificate and usage
for Authentication -->
    </xs:complexType>
    <!--OSCI Policy Asserstions-->
    <!--Policy qualified Timestamp Servcie available-->
  </xs:element>
  <!--Poliy Assertion carrying Endpoints X509Certificates-->
  <xs:element name="X509CertificateAssertion">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="wsp:All"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <!--Policy, when qualified TSP service can be requested form this node-->
  <xs:element name="QualTspAssertion">
    <xs:complexType>
      <xs:attribute name="PolicyRef" type="xs:anyURI"/>
    </xs:complexType>
  </xs:element>
  <!--Policy if and how MsgTimeStamps:OsoleteAfter is handled-->
  <xs:element name="ObsoleteAfterAssertion">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="MsgRetainDays" type="xs:positiveInteger"/>
        <xs:element name="WarningBeforeMsgObsolete" type="xs:positiveInteger"
minOccurs="0"/>
      </xs:sequence>
      <xs:attribute name="PolicyRef" type="xs:anyURI"/>
    </xs:complexType>
  </xs:element>
  <!--Poliy for MakeConnection: Response Retention Days-->
  <xs:element name="MsgRetainDays" type="xs:positiveInteger"/>
  <!--Enumeration for possible X509 Token Usages-->
  <xs:attribute name="TokenUsage">
    <xs:simpleType>
      <xs:restriction base="xs:anyURI">
        <xs:enumeration
value="http://www.osci.eu/common/names/TokenUsage/e2eContentEncryption"/>
        <xs:enumeration
value="http://www.osci.eu/common/names/TokenUsage/TransportEncryption"/>
        <xs:enumeration
value="http://www.osci.eu/common/names/TokenUsage/ReceiptSigning"/>
        <xs:enumeration
value="http://www.osci.eu/common/names/TokenUsage/TSPSigning"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:attribute>
  <!--Opaque Body Type - not used-->
  <!--Policy maximum accepted Message size and Frequency per hour-->
  <xs:element name="AcceptedMsgLimits">
```

```
3533      <xs:complexType>
3534        <xs:sequence>
3535          <xs:element name="MaxSize" type="xs:positiveInteger"/>
3536          <xs:element name="MaxPerHour" type="xs:positiveInteger"/>
3537        </xs:sequence>
3538      </xs:complexType>
3539    </xs:element>
3540    <xs:complexType name="MessageBody">
3541      <xs:sequence>
3542        <xs:any namespace="##any" minOccurs="0" maxOccurs="unbounded"/>
3543      </xs:sequence>
3544    </xs:complexType>
3545  </xs:schema>
```

Appendix B. Example: OSCI Endpoint Metadata Instance

This example is a policy instance of the schema explained in chapter [10.2]. The encryption and signature certificates exposed in this policy are addressed by URI refererences; according to [WSS] they could also be embedded it this policy file itself in base64Binary format.

This enpoint exposes different encryption and signature certificates for the MsgBox and Recipient / UltimateRecipient instances. The [ObsoleteAfter] property is handled by this endpoint, while a service for qualified timestamps is not offered.

For readability of policies used in the OSCI Transport context, it is strongly RECOMMENDED generally to use the **`wsu:id`** attribute values highligthed **bold** in this example, as these policy parts and certificates are referenced by other policies or service instances like a STS (i.e., the latter needs access to the endpoint encryption certificate for appropriate SAML token encryption).

```
<?xml version="1.0" encoding="UTF-8"?>
<!--- OSCI specifc endpoint metadata / policies -->
<wsp:Policy Name="ExampleEndpointOSCIPolicy"
xsi:schemaLocation="http://schemas.xmlsoap.org/ws/2004/09/policy
http://schemas.xmlsoap.org/ws/2004/09/policy/ws-policy.xsd"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd" xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
xmlns:wspmtom="http://schemas.xmlsoap.org/ws/2004/09/policy/optimizedmimeserializat
ion" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"
xmlns:fimac="urn:de:egov:names:fim:1.0:authenticationcontext"
xmlns:osci="http://www.osci.eu/ws/2008/05/transport.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <wsp:All>

    <wsp:Policy wsu:id="X509CertificateAssertion">
      <osci:X509CertificateAssertion>
        <wsp:ALL>
          <wsse:SecurityTokenReference wsu:id="UltimateRecipientEncCert"
wsse:Usage="http://www.osci.eu/2008/05/common/names/TokenUsage/e2eContentEncryption
" osci:Role="http://www.w3.org/2003/05/soap-envelope/role/ultimateReceiver">
            <wsse:Reference URI="REPLACE_WITH_ACTUAL_URL to UltimateRecipientEncCert"
ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-
profile-1.0#X509v3"/>
          </wsse:SecurityTokenReference>
          <wsse:SecurityTokenReference wsu:id="RecipientSigCert"
wsse:Usage="http://www.osci.eu/2008/05/common/names/TokenUsage/ReceiptSigning"
osci:Role="http://www.osci.eu/ws/2008/05/transport/role/Recipient">
            <wsse:Reference URI="REPLACE_WITH_ACTUAL_URL to RecipientSigCert"
ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-
profile-1.0#X509v3"/>
          </wsse:SecurityTokenReference>
          <wsse:SecurityTokenReference wsu:id="MsgBoxEncCert"
wsse:Usage="http://www.osci.eu/2008/05/common/names/TokenUsage/TransportEncryption"
osci:Role="http://www.osci.eu/2008/05/common/names/role/MsgBox">
            <wsse:Reference URI="REPLACE_WITH_ACTUAL_URL to MsgBoxEncCert"
ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-
profile-1.0#X509v3"/>
          </wsse:SecurityTokenReference>
          <wsse:SecurityTokenReference wsu:id="MsgBoxSigCert"
wsse:Usage="http://www.osci.eu/2008/05/common/names/TokenUsage/ReceiptSigning"
osci:Role="http://www.osci.eu/2008/05/common/names/role/MsgBox">
            <wsse:Reference URI="REPLACE_WITH_ACTUAL_URL to MsgBoxSigCert"
ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-
profile-1.0#X509v3"/>
          </wsse:SecurityTokenReference>
        </wsp:ALL>
      </osci:X509CertificateAssertion>
    </wsp:Policy>

    <wsp:Policy wsu:id="ServicesAssertion">
      <osci:ObsoleteAfterAssertion
PoliyRef="http://www.OSCIExmapleEndPoint/MsgRetainPolicy.htm">
```

```
        <osci:MsgRetainDays>7</osci:MsgRetainDays>
      </osci:ObsoleteAfterAssertion>
    </wsp:Policy>

    <wsp:Policy wsu:id="AuthLevelPolicy">

  <fimac:Authentication>urn:de:egov:names:fim:1.0:securitylevel:high</fimac:Authenti
cation>

  <fimac:Registration>urn:de:egov:names:fim:1.0:securitylevel:veryhigh</fimac:Regist
ration>
    </wsp:Policy>
  </wsp:All>
</wsp:Policy>
```

Listing 1: ExampleEndpointOSCIPolicy.xml

Appendix C. Example Signature Element

For illustration, following example is given for an instance of such a signature element:

```
<ds:Signature Id="uuid:E57C0006-A629-5767-ED32-2667F1512912">
  <ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm=
  "http://www.w3.org/2001/10/xml-exc-c14n#" />
    <ds:SignatureMethod Algorithm=
"http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
    <ds:Reference URI="#uuid:97544A28-F042-9457-3286-DD37F6FF7FEA">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <ds:DigestValue>DQrljZZVeewWoXLzLLi/uPqESY2fGscAjVLBXpjKEnM=</ds:DigestValue>
    </ds:Reference>
<ds:Reference Id="uuid:4422AB49-BF3E-8521-BD1D-820F2160DDC6"
  Type="http://uri.etsi.org/01903/v1.1.1/#SignedProperties"
  URI="#uuid:5A075139-52E8-CF5E-3A1B-F54B6B1F1025">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <ds:DigestValue >RjwjBl2TBumKSvG05Jgelzz6jlilA3t7GUxikLaa8io=</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>FrPlHt0v/Njnk...8JZV/LE141aSTcLyBxBQ==</ds:SignatureValue>
  <ds:KeyInfo >
    <ds:X509Data >
      <ds:X509Certificate>MIIDHjCCAgagAwIBAAIER4...YQya8Q==</ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
  <ds:Object>
    <xades:QualifyingProperties Target="#uuid:E57C0006-A629-5767-ED32-2667F1512912">
      <xades:SignedProperties>
        <xades:SignedSignatureProperties
Id="uuid:5A075139-52E8-CF5E-3A1B-F54B6B1F1025">
          <xades:SigningTime>2008-01-17T18:57:27</xades:SigningTime>
          <xades:SigningCertificate>
            <xades:Cert>
              <xades:CertDigest>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue >0uGTT8Gg..oXRjpsKp9BMVBaYid7kzsa4=</ds:DigestValue>
```

```
            </xades:CertDigest>
            <xades:IssuerSerial>
              <ds:X509IssuerName>CN=Apitzsch, OU=QA, O=waycony, L=Hamburg, C=DE
              </ds:X509IssuerName>
              <ds:X509SerialNumber >1200577645</ds:X509SerialNumber>
            </xades:IssuerSerial>
          </xades:Cert>
        </xades:SigningCertificate>
      </xades:SignedSignatureProperties>
    </xades:SignedProperties>
    <xades:UnsignedProperties>
      <xades:UnsignedSignatureProperties>^
          <xades:SignatureTimeStamp>
          <ds:CanonicalizationMethod Algorithm=
            "http://www.w3.org/2001/10/xml-exc-c14n#"/>
          <xades:EncapsulatedTimeStamp>0uGKT8Gg..oXRjpsKp9BMVBaYid
          </xades:EncapsulatedTimeStamp>
          </xades:SignatureTimeStamp>
      </xades:UnsignedSignatureProperties>
    </xades:UnsignedProperties>
  </xades:QualifyingProperties>
 </ds:Object>
</ds:Signature>
```

Listing 2: Example XML Signature

Appendix D. Acknowledgements

Following people having contributed temporarely or during the whole specification process to the OSCI Transport 2 concepts and documents are gratefully acknowledged:

Requirements, Architecture and Specification Working Groups

Jörg Apitzsch (bos), Ingo Beyer (PC-Ware), Thomas Biere (BSI), Oliver Böhm (Fraunhofer ISST), Nils Büngener (bos), Dr. Peter Dettling (IBM Deutschland), Jan Füssel (cit), Clemens Gogolin (PTB), Golo Hoffmann (procilon), Marc Horstmann (bos), Christoph Karich (Hochschule Harz), Daniel Koszior (PC-Ware), Harald Krause (Dataport), Arnold Külper (DVZ Mecklenburg-Vorpommern), Raik Kuhlisch (Fraunhofer ISST), Ralf Lindemann (bos), Dr. Klaus Lüttich (bos), Fabian Meiswinkel (Microsoft Deutschland), Lutz Nentwig (Fraunhofer ISST), Lars Nitzsche (procilon), Torsten Rienaß (procilon), Martin Schacht (Microsoft Deutschland), Thilo Schuster (cit),Janos Schwellach (bos), Prof. Dr.-Ing. Hermann Strack (Hoschule Harz), Dr. Hamed Tabrizi (bos), Lutz Vorwerk (IZN Niedersachsen), Sascha Weinreuter (cit), Mario Wendt (Microsoft Deutschland)

Approval Instance

Members of the Architecture and Specification Working Group and:

Marcel Boffo (LDI Rheinland-Pfalz), Carlheinz Braun (DPMA), Christoph Damm (Staatskanzlei Sachsen), Steffen Düring (UBA), Joachim Gerber (INFORA), Reto Giger (Schweizer Post), Jens Habermann (LDS Düsseldorf), Renée Hinz (UBA), Wolfgang Klebsattel (DLR), Andreas Kraft (PBEG), Svea Lahn (HSH), Dr. Christian Mrugalla (BMI), Dr. Bernhard Paul (IBM Deutschland), Maren Pohl (HABIT), Anja Riekenberg (Hannit), Martin Rost (ULD Kiel), Alexander Spohn (ITDZ), Frank Steimke (OSCI Leitstelle), Andrea Steinbeck (HSH),Heiko Thede (DVZ Mecklenburg-Vorpommern), Joachim Wille (SAP Deutschland)