



# Telecom SOA Requirements Version 1.0

## Committee Draft 02

8 June 2010

### Specification URIs:

#### This Version:

<http://docs.oasis-open.org/soa-tel/t-soa-req1.0/cd02/t-soa-req-01-cd-02.html>  
<http://docs.oasis-open.org/soa-tel/t-soa-req1.0/cd02/t-soa-req-01-cd-02.pdf> (Authoritative)  
<http://docs.oasis-open.org/soa-tel/t-soa-req1.0/cd02/t-soa-req-01-cd-02.doc>

#### Previous Version:

<http://docs.oasis-open.org/soa-tel/t-soa-req1.0/cd01/t-soa-req-01-cd-01.html>  
<http://docs.oasis-open.org/soa-tel/t-soa-req1.0/cd01/t-soa-req-01-cd-01.pdf> (Authoritative)  
<http://docs.oasis-open.org/soa-tel/t-soa-req1.0/cd01/t-soa-req-01-cd-01.doc>

#### Latest Version:

<http://docs.oasis-open.org/soa-tel/t-soa-req1.0/t-soa-req-01.html>  
<http://docs.oasis-open.org/soa-tel/t-soa-req1.0/t-soa-req-01.pdf> (Authoritative)  
<http://docs.oasis-open.org/soa-tel/t-soa-req1.0/t-soa-req-01.doc>

### Technical Committee:

OASIS SOA for Telecom (SOA-Tel) TC

### Chair(s):

Enrico Ronco, [enrico.ronco@telecomitalia.it](mailto:enrico.ronco@telecomitalia.it)

### Editor(s):

Enrico Ronco, [enrico.ronco@telecomitalia.it](mailto:enrico.ronco@telecomitalia.it)

### Related work:

This specification replaces or supersedes:

- N/A

This specification is related to:

- [OASIS Telecom Use Cases and Issues Version 1.0](#)

### Declared XML Namespace(s):

- N/A

### Abstract:

This document is the second deliverable produced within the OASIS SOA-TEL TC and has the objective of collecting requirements related to technical issues and gaps of SOA standards (specified by OASIS and other SDOs) utilized within the context of Telecoms. Such technical issues are documented in SOA-TEL's TC first deliverable "Telecom Use Cases and Issues, v.1.0".

For each of the issues within the "Telecom Use Cases and Issues, v.1.0", specific requirements are provided within this document. Where possible, non prescriptive solution proposals to the identified issues and requirements are also described, in order to possibly assist those Technical Committees (within OASIS and other SDOs) responsible for the development and maintenance of the SOA related standards.

**Status:**

This document was last revised or approved by the OASIS SOA for Telecom (SOA-Tel) TC on the above date. The level of approval is also listed above. Check the “Latest Version” or “Latest Approved Version” location noted above for possible later revisions of this document.

Technical Committee members should send comments on this specification to the Technical Committee’s email list. Others should send comments to the Technical Committee by using the “Send A Comment” button on the Technical Committee’s web page at <http://www.oasis-open.org/committees/soa-tel/>.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Technical Committee web page (<http://www.oasis-open.org/committees/soa-tel/ipr.php>).

The non-normative errata page for this specification is located at <http://www.oasis-open.org/committees/soa-tel/>.

---

## Notices

Copyright © OASIS® 2009-2010. All Rights Reserved.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The names "OASIS", "SOA-TEL" are trademarks of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see <http://www.oasis-open.org/who/trademark.php> for above guidance.

---

# Table of Contents

1	Introduction.....	7
1.1	Terminology.....	7
1.2	Normative References.....	8
1.3	Non Normative References.....	8
2	Requirements on Intermediaries.....	9
2.1	Requirements on Transaction Endpoints Specification.....	9
2.1.1	Identification of Use Case.....	9
2.1.2	Requirement(s).....	9
2.1.3	Description.....	9
2.1.4	Solution proposals.....	10
2.2	Requirements on WS-Notification.....	13
2.2.1	Identification of Use Case.....	13
2.2.2	Requirement(s).....	13
2.2.3	Description.....	13
2.2.4	Solution proposals.....	14
2.3	Requirements on SOAP.....	20
2.3.1	Identification of Use Case.....	20
2.3.2	Requirement(s).....	21
2.3.3	Description.....	21
2.3.4	Solution proposals.....	21
3	Requirements on Security.....	24
3.1	Requirements on Security Token Correlation.....	24
3.1.1	Identification of Use Case.....	24
3.1.2	Requirement(s).....	24
3.1.3	Description.....	24
3.1.4	Solution proposals.....	24
3.2	SAML Name Identifier Request.....	27
3.2.1	Identification of Use Case.....	27
3.2.2	Requirement(s).....	27
3.2.3	Solution proposal.....	28
3.3	SAML Attribute Management Request.....	30
3.3.1	Identification of Use Case.....	30
3.3.2	Requirement(s).....	30
3.3.3	Description.....	31
3.3.4	Solution proposal.....	31
3.4	User ID Forwarding.....	34
3.4.1	Scenario/context.....	34
3.4.2	Identification of Use Case.....	34
3.4.3	Requirement(s).....	34
3.4.4	Description.....	34
3.4.5	Solution proposals.....	35
4	Requirements on Management.....	37
4.1	Cardinality of a Service Interface.....	37

4.1.1	Identification of Use Case.....	37
4.1.2	Requirement(s).....	37
4.1.3	Description .....	38
4.1.4	Solution proposals.....	38
4.2	Requirements on Metadata .....	38
4.2.1	Identification of Use Case.....	38
4.2.2	Requirement(s).....	39
4.2.3	Description .....	39
4.2.4	Solution proposals.....	39
5	Requirements on SOA collective standards usage .....	40
5.1	Common Patterns for Interoperable Service Based Communications.....	40
5.1.1	Identification of Use Case.....	40
5.1.2	Requirement(s).....	40
5.1.3	Description .....	40
6	Conformance.....	41
	Appendix A. Acknowledgements.....	43
	Appendix B. SOA-TEL Requirements .....	44

---

## Table of Figures

Figure 1: Example for SOAP nodes interaction (1) .....	11
Figure 2: Example for SOAP nodes interaction (2) .....	12
Figure 3: Example for SOAP nodes interaction (3) .....	13
Figure 4: SAML Name Identifier request-response use case: pictorial representation.....	27
Figure 5: SAML Attribute Management request-response use case: pictorial representation.....	31
Figure 6: TM Forum SDF Reference Model .....	38

---

# 1 Introduction

Part of the work being undertaken by the OASIS SOA-TEL TC is to understand how SOA-related specifications and standards are used within the scope of the telecommunications environment and determine if there are any issues when used in this manner.

This is the second deliverable of the SOA-TEL TC, and its objective is to collect requirements to address technical issues and gaps of SOA standards (specified by OASIS and other SDOs) utilized within the context of Telecoms. Such issues are documented in SOA-TEL's TC first deliverable "Telecom Use Cases and Issues, v.1.0".

For each of the issues within such document, specific requirements are provided. Where possible, non prescriptive solution proposals to the identified issues and requirements are also described, in order to possibly assist those Technical Committees (within OASIS and other SDOs) responsible for the development and maintenance of the SOA related standards.

For each of the issues identified within "Telecom Use Cases and Issues, v.1.0", a section composed of

- "References",
- "Requirement",
- "Description",
- and "Proposed solution"

is included in this Requirements document.

In order to facilitate future activities, each requirement is identified by means of a reference, with the syntax [SOA-TEL Req. x.y].

The document is organized in the following sections:

- Section 2, Issues on "Intermediaries";
- Section 3, Issues on "Security";
- Section 4, Issues on "Management";
- Section 5, Issues on "SOA collective standards usage".

Moreover, Appendix B, SOA-TEL Requirements, groups all exposed requirements within one single view.

The next steps related to this activity will be taken within the OASIS Telecom Member Section. Most likely, issues and related requirements will be grouped according to categories, and sent and presented to the TCs or Working Groups considered as "owners" of the affected specifications, in order to verify if such groups will want to analyze them and provide their solution. Other alternatives may also be evaluated on a case by case approach. Nevertheless the solution of identified issues and the addressing of the requirements hereafter listed is not to be considered as part of SOA-TEL's TC Charter.

## 1.1 Terminology

The key words "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]**.

## 43 1.2 Normative References

- 44 [RFC2119] S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*,  
45 <http://www.ietf.org/rfc/rfc2119.txt>, IETF RFC 2119, March 1997.  
46
- 47 [WSDL 1.1] W3C Note (15 March 2001): "Web Services Description Language (WSDL)  
48 1.1". <http://www.w3.org/TR/2001/NOTE-wsdl-20010315>.  
49
- 50 [SOAP 1.2] W3C SOAP v.1.2, available at <http://www.w3.org/TR/soap12-part1/>  
51
- 52 [SOA-TEL 1.0] OASIS Committee Specification 01, "Telecom SOA Use Cases and Issues  
53 Version 1.0", March 2010. <http://docs.oasis-open.org/soa-tel/t-soa-uci/v1.0/cs01/t-soa-uc-cs-01.html>  
54
- 55
- 56 [WS-N 1.3] OASIS Standard, "Web Services Base Notification 1.3 (WS-BaseNotification)  
57 Version 1.3", October 2006. [http://docs.oasis-open.org/wsn/wsn-ws\\_base\\_notification-1.3-spec-os.htm](http://docs.oasis-open.org/wsn/wsn-ws_base_notification-1.3-spec-os.htm).  
58
- 59
- 60 [WS-A 1.0] W3C Web Services Addressing 1.0 – Core W3C Recommendation 9 May  
61 2006, <http://www.w3.org/TR/2006/REC-ws-addr-core-20060509/>.  
62
- 63 [WS-S 1.1] OASIS Standard, "Web Services Security Specification Version 1.1",  
64 February 2006. <http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SOAPMessageSecurity.pdf>  
65
- 66
- 67 [WSDM-MOWS] OASIS Standard, "Web Services Distributed Management: Management of  
68 Web Services (WSDM-MOWS) Version 1.1", August 2006. <http://docs.oasis-open.org/wsdm/wsdm-mows-1.1-spec-os-01.htm>  
69
- 70
- 71 [SOA RM 1.0] OASIS Standard, "OASIS Reference Model for Service Oriented Architecture  
72 1.0", October 2006. <http://docs.oasis-open.org/soa-rm/v1.0/soa-rm.pdf>  
73
- 74 [SCA Assembly 1.1] OASIS Committee Draft, "Service Component Architecture Assembly Model  
75 Specification Version 1.1", January 2010. <http://docs.oasis-open.org/opencsa/sca-assembly/sca-assembly-1.1-spec.pdf>  
76
- 77
- 78 [SOA RA 1.0] OASIS Committee Draft 01 Public Review 01, "Reference Architecture for  
79 Service Oriented Architecture Version 1.0", April 2008. <http://docs.oasis-open.org/soa-rm/soa-ra/v1.0/soa-ra-pr-01.pdf>  
80
- 81
- 82 [WSDL 2.0] W3C Web Services Description Language (WSDL) Version 2.0 Part 0:  
83 Primer, <http://www.w3.org/TR/2007/REC-wsdl20-primer-20070626/>, June  
84 2007
- 85
- 86 [SAML 2.0] OASIS Standard, "Security Assertion Markup Language (SAML) Version  
87 2.0", March 2005. <http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf>  
88

## 89 1.3 Non Normative References

90 N/A

91



---

## 2 Requirements on Intermediaries

Some existing specifications used by Service Oriented Architectures do not allow for the presence of intermediaries in message exchanges. The lack of standards for intermediaries has led to workarounds and proprietary solutions. This section develops the requirements for intermediaries in message exchanges.

OASIS SOA-TEL TC considers that addressing the specific requirements provided in this section may be the first step for a more general revision of the SOA specifications in order to extend their coverage to include the management of intermediaries.

### 2.1 Requirements on Transaction Endpoints Specification

#### 2.1.1 Identification of Use Case

There is no standard way to specify in a message that is subject to a process or transaction, the end point to which the message should be sent at the end of the process or transaction.

The lack of endpoint specification in messages is more fully documented in [SOA-TEL 1.0], 3.1 Transaction Endpoints Specification.

#### 2.1.2 Requirement(s)

##### Req. 1

The WS Addressing specifications, [WS-A 1.0], must include additional fields (in addition to the ones already present) containing remote destinations to which reply messages must be sent.

- The sender of a message must assign the fields when it wants to specify the destination for the reply message, but the node that has to use such destination information (i.e. the node that has to send the reply message) may not necessarily be the direct receiver of the request message.
- The receiver of a message, which needs of information on the endpoint destination to which send a reply message, can obtain the information by these additional fields.
- The receiver of a message has to forward to the next receiver all the additional destinations (present in these additional fields) that it does not use.

#### 2.1.3 Description

The [WS-A 1.0] must include additional information to indicate nodes to which messages replies should be sent (in addition to the one already present).

Specific endpoints should be inserted when the message is part of a transaction involving more participants. Such endpoints must be forwarded, through the chain of invocations, to those nodes that will need to use these endpoints.

The generic node that starts a transaction should be able to specify endpoints for the nodes following in the transaction, in addition to the (already available) “reply\_to” endpoint for the message’s direct receiver.

In complex scenarios involving more than 3 nodes, the generic node N that receives a message may not be conscious of the specific transaction of which it is part of, or of other participant nodes, but could obtain the endpoint to which it must send a reply message by fetching such new proposed endpoint element.

132 Moreover, the current “reply to” element within the WS-A specification could not be utilized for this  
133 objective because even the direct sender to node N may not be aware of the final destination for the  
134 message.

## 135 2.1.4 Solution proposals

136 The following text is provided in order to illustrate some possible ways to address the Requirement. They  
137 are suggestions and are by no means to be considered as mandatory, as other possible options could be  
138 identified which are not represented hereafter.

139

140 To the best knowledge within OASIS SOA-TEL TC, the requirements presented hereafter could be  
141 addressed by the W3C Web Services Addressing (WS-A) WG, which by the way is in status “Completed”.

142

143 The WS-Addressing v1.0 specification [WS-A 1.0] defines the following elements:

144

145	<code>wsa:To&gt;xs:anyURI&lt;/wsa:To&gt; ?</code>
146	<code>&lt;wsa:From&gt;wsa:EndpointReferenceType&lt;/wsa:From&gt; ?</code>
147	<code>&lt;wsa:ReplyTo&gt;wsa:EndpointReferenceType&lt;/wsa:ReplyTo&gt; ?</code>
148	<code>&lt;wsa:FaultTo&gt;wsa:EndpointReferenceType&lt;/wsa:FaultTo&gt; ?</code>
149	<code>&lt;wsa:Action&gt;xs:anyURI&lt;/wsa:Action&gt;</code>
150	<code>&lt;wsa:MessageID&gt;xs:anyURI&lt;/wsa:MessageID&gt; ?</code>
151	<code>&lt;wsa:RelatesTo RelationshipType="xs:anyURI"?&gt;xs:anyURI&lt;/wsa:RelatesTo&gt; *</code>
152	<code>&lt;wsa:ReferenceParameters&gt;xs:any*&lt;/wsa:ReferenceParameters&gt; ?</code>

153

154 Another element could be added to contain a “remote” endpoint reference, named for example

155

156	<code>&lt;wsa:RemoteReplyTo&gt; wsa:EndpointReferenceType&lt;/wsa:RemoteReplyTo&gt; *.</code>
-----	---

157

158 It should be possible to add more RemoteReplyTo elements, in a LIFO (Last In First Out) criteria.

159

160 The generic receiver can use the last inserted endpoint and delete the element.

161

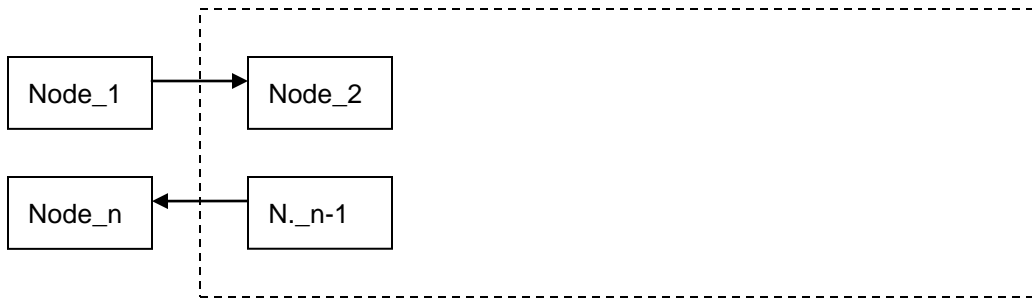
162 The following example is provided.

163

164 Suppose that *node\_1* calls *node\_2*.

165 *node\_1* states that the endpoint for the response is *node\_n*, but it doesn't know which node will be  
166 sending the final response to *node\_n* at the end of the transaction, so it inserts the information (*node\_n*  
167 endpoint) in the RemoteReply element, not in ReplyTo one. Figure 1 illustrates the example.

168



169  
 170  
 171  
 172  
 173  
 174  
 175  
 176

Figure 1: Example for SOAP nodes interaction (1)

The following is an example of the resulting message (in red color the proposed addition to the WS-A specification).

```

<soap:Envelope...>
  <soap:Header>
    <wsa:To> http://host_a/node_2 </wsa:To>
    <wsa:RemoteReplyTo>
      <wsa:Address>
        http://host_b/node_n
      </wsa:Address>
    </wsa:RemoteReplyTo>
    ...
  </soap:Header>
  <soap:Body>
    ...
  </soap:Body>
</soap:Envelope>
  
```

177  
 178  
 179  
 180  
 181  
 182  
 183  
 184

Suppose now that *node\_i* in the transaction, calling *node\_i+1*, starts a nested transaction (with *node\_j* as final destination) in the main transaction. Also in this case, *node\_i* does not know which will produce the response for the *node\_j*, so it adds a RemoteReply element, to the message. Figure 2 illustrates the example.

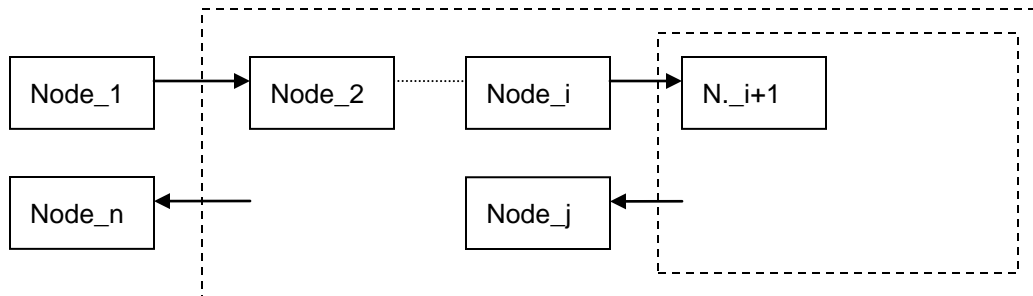


Figure 2: Example for SOAP nodes interaction (2)

185  
186  
187  
188  
189

The resulting message should be the following.

```

<soap:Envelope...>
  <soap:Header>
    <wsa:To> http://host_c/node_i+1 </wsa:To>
    <wsa:RemoteReplyTo>
      <wsa:Address>
        http://host_d/node_j
      </wsa:Address>
    </wsa:RemoteReplyTo>
    <wsa:RemoteReplyTo>
      <wsa:Address>
        http://host_b/node_n
      </wsa:Address>
    </wsa:RemoteReplyTo>
    ...
  </soap:Header>
  <soap:Body>
    ...
  </soap:Body>
</soap:Envelope>
  
```

190  
191  
192  
193  
194  
195  
196  
197  
198

Suppose now that *node<sub>j-1</sub>* ends the nested transaction.

*node<sub>j-1</sub>* needs a reply destination, so it fetches the endpoint by the first RemoteReplyTo element, obtaining the information "http:// host\_d/node<sub>j</sub>"; it then deletes the element in the header and replies to *node<sub>j</sub>*.

*node<sub>n-1</sub>*, last node of the main transaction, should perform in the same way with the remaining RemoteReplyTo element. Figure 3 illustrates the example.

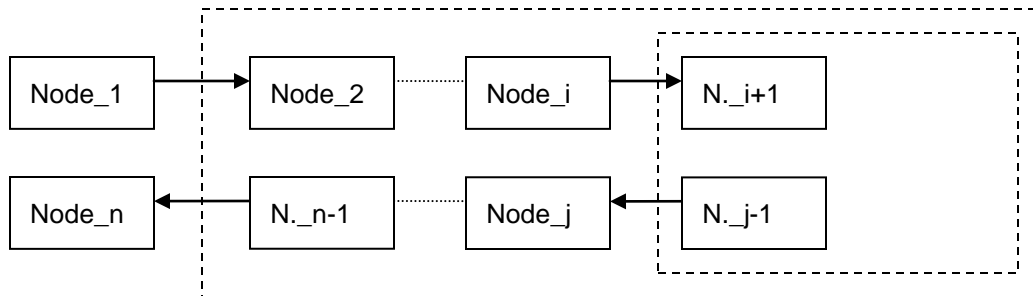


Figure 3: Example for SOAP nodes interaction (3)

## 2.2 Requirements on WS-Notification

### 2.2.1 Identification of Use Case

If adopting the WS-Notification [WS-N 1-3] specification, in presence of intermediaries, there is no formal way for the Provider to specify the endpoint to which the final notification should be sent.

Refer to [SOA-TEL 1.0], 3.2 of the SOA-TEL “Telecom Use Cases and Issues” document, in which the technical issue is documented.

### 2.2.2 Requirement(s)

#### Req. 2

The WS-Notification specification must provide a mechanism to describe and regulate a scenario in which one or more intermediaries are present; it must standardize the terminology, concepts, operations, WSDL and XML needed to express the roles of the intermediaries (involved in publish and subscribe Web services for notification message exchange).

According to the WS-Notification terminology, the standard must be extended and modified so that:

- a *Subscriber* can require a *Subscription* to a *NotificationProducer* also in the case they do not communicate directly but do so by means of one or more intermediaries;
- likewise a *NotificationProducer* can send a *Notification* to a *NotificationConsumer* also in the case that they do not communicate directly, but by means of one or more intermediaries.

### 2.2.3 Description

The WS-Notification specification must provide a well specified mechanism whereby a Subscriber can interact (by means of “subscribe”, “unsubscribe” and the other provided operations) with a NotificationProducer also in presence of one or more intermediaries between itself and the NotificationProducer.

Moreover the WS-Notification specification must provide a well specified mechanism by which a NotificationProducer can send notifications to a given NotificationConsumer also via one or more intermediaries.

In the new context, the Subscriber must be able to send a subscription message (different from the ones allowed by the current specification) to an intermediary; the intermediary must be able to request the subscription to the NotificationProducer or to send the request to the next intermediary. As a consequence an intermediary can receive a subscription request from another intermediary.

233 Moreover the new subscription response message must be managed and forwarded by intermediaries in  
234 a similar way.

235  
236 Conversely, the NotificationProducer must be able to send a notification addressed to a  
237 NotificationConsumer to an intermediary, and this intermediary must be able to forward the notification to  
238 the NotificationConsumer or to the next intermediary. In consequence of that an intermediary can receive  
239 a notification from another intermediary.

240  
241 This requirement is closely connected to the requirement over WS-Addressing, described in Section 2.1  
242 of this document (Requirements on Transaction Endpoints Specification) for two reasons:

- 243 • the two requirements introduce and regulate "intermediaries management" in the WS-Addressing and  
244 WS-Notification specifications
- 245 • WS-Notification specification characterizes and identifies the actors (such as Subscriber and  
246 NotificationProducer) by means of the WS-Addressing standard.

## 247 **2.2.4 Solution proposals**

248 The following text is provided in order to illustrate some possible ways to address the requirement. They  
249 are suggestions and are by no means to be considered as mandatory, as other possible options could be  
250 identified which are not represented hereafter.

251 To the best knowledge within OASIS SOA-TEL TC, the requirements presented hereafter could be  
252 addressed by the OASIS WS-Notification Technical Committee (WSN TC), which by the way is in status  
253 "Completed", or possibly, by the W3C Web Services Addressing (WS-A) WG, which by the way is as well  
254 in status "Completed".

255 Another Working Group potentially interested to receive this requirement is W3C Resource Access since  
256 the topic dealt by the specifications (WS-Transfer, WS-ResourceTransfer, WS-Enumeration, WS-  
257 MetadataExchange and WS-Eventing Member Submissions) for which this group is responsible may  
258 potentially solve the present issues with WS-N specification.

259  
260 There are several approaches to solve the requirement: the solution to adopt depends on the chosen  
261 perspective, on the use cases that are to be covered, and on the scope to assign to the new specification.

262 Two different lines of solution, not antithetical, but complementary, are provided below. In the first  
263 proposal the intermediary plays an active part in the notification services, while the second proposal is  
264 more general, and is based on the fact that WS-Notification is supported by WS-Addressing.

265  
266 **First proposal** (intermediary plays an active part in the notification services)

267 The WS-Notification specification should define a new role in addition to the ones already defined  
268 (NotificationConsumer, NotificationProducer, SubscriptionManager, Subscriber).

269 The new role could be named, for example, "Intermediary", and its description could be:

- 270 • *an entity acting on behalf of a Subscriber; it receives a subscription request and asks for the*  
271 *subscription to the NotificationConsumer specified in the request, or forwards the request the next*  
272 *Intermediary;*
- 273 • *an entity acting on behalf of a NotificationProducer; it receives a notification and sends it to the*  
274 *NotificationConsumer specified in the notification message, or forwards the request to the next*  
275 *Intermediary.*

276 To be noted that an Intermediary node could contemporarily have both behaviours: acting on behalf of a  
277 *Subscriber* to request a subscription to a *NotificationProducer*, and acting on behalf of a Notification  
278 Producer to send a notification message to a *Subscriber*.

279

280 The protocol should be extended in such as way to define a new message exchange pattern in which  
281 even the Intermediary behaviour is comprised.

282

283 The syntax of the subscription request and that of the notification should be extended so that it becomes  
284 possible to specify, in the new messages, one or more intermediary destinations and the final destination.

285

286 For example, for the subscription operation, if the Subscriber knows the NotificationProvider location, it  
287 can make a subscription request in which it inserts an endpoint reference element for the  
288 NotificationProvider, and then sends the message to the Intermediary; the Intermediary consumes (reads  
289 and deletes) the reference and so it is able to send a subscribe request to the NotificationProvider.

290 In the subscription request, the endpoint reference of the Intermediary to which notifications should be  
291 sent, could be also included.

292 The subscribe message could be as the following:

293

```

<s:Envelope ... >
  <s:Header>
    <wsa:Action>
      http://docs.oasis-open.org/wsn/bw-2/Intermediary/SubscribeRequest
    </wsa:Action>
    ...
  </s:Header>
  <s:Body>
    <wsnt:Subscribe>
      <wsnt:ConsumerReference>
        <wsa:Address>
          http://www.example.org/NotificationConsumer
        </wsa:Address>
      </wsnt:ConsumerReference>
      <wsnt:ProducerReference>
        <wsa:Address>
          http://www.example.org/NotificationProducer
        </wsa:Address>
      </wsnt:ProducerReference>
      <wsnt: IntermediaryReference>
        <wsa:Address>
          http://www.example.org/Intermediary
        </wsa:Address>
      </wsnt: IntermediaryReference>
      <wsnt:Filter>
        <wsnt:TopicExpression Dialect=
"http://docs.oasis-open.org/wsn/t-1/TopicExpression/Simple">
          ncex:SomeTopic
        </wsnt:TopicExpression>
        <wsnt:MessageContent
          Dialect="http://www.w3.org/TR/1999/REC-xpath-19991116">
          boolean(ncex:Producer="15")
        </wsnt:MessageContent>
      </wsnt:Filter>
      <wsnt:InitialTerminationTime>
        2005-12-25T00:00:00.00000Z
      </wsnt:InitialTerminationTime>
    </wsnt:Subscribe>
  </s:Body>
</s:Envelope>

```

294  
295  
296  
297  
298  
299

The Intermediary receives the above message and makes a subscription request to the notification consumer with the following message:



```

<s:Envelope ... >
  <s:Header>
    <wsa:Action>
      http://docs.oasis-open.org/wsn/bw-
2/NotificationProducer/SubscribeRequest
    </wsa:Action>
    ...
  </s:Header>
  <s:Body>
    <wsnt:Subscribe>
      <wsnt:ConsumerReference>
        <wsa:Address>
          http://www.example.org/NotificationConsumer
        </wsa:Address>
      </wsnt:ConsumerReference>
      <wsnt: IntermediaryReference>
        <wsa:Address>
          http://www.example.org/Intermediary
        </wsa:Address>
      </wsnt: IntermediaryReference>
      <wsnt:Filter>
        <wsnt:TopicExpression Dialect=
"http://docs.oasis-open.org/wsn/t-1/TopicExpression/Simple">
          npex:SomeTopic
        </wsnt:TopicExpression>
        <wsnt:MessageContent
          Dialect="http://www.w3.org/TR/1999/REC-xpath-19991116">
          boolean(ncex:Producer="15")
        </wsnt:MessageContent>
      </wsnt:Filter>
      <wsnt:InitialTerminationTime>
        2005-12-25T00:00:00.00000Z
      </wsnt:InitialTerminationTime>
    </wsnt:Subscribe>
  </s:Body>
</s:Envelope>

```

300  
301

302 The notification message could be the similar to these defined with the current specification, but sent by  
303 the NotificationProducer to the Intermediary rather than directly to the NotificationConsumer, as showed  
304 in the next figure; in this message the final destination should be present.

```

<s:Envelope ... >
  <s:Header>
    <wsa:Action>
      http://docs.oasis-open.org/wsn/bw-2/Intermediary/Notify
    </wsa:Action>
    ...
  </s:Header>
  <s:Body>
    <wsnt:Notify>
      <wsnt:NotificationMessage>
        <wsnt:SubscriptionReference>
          <wsa:Address>
            http://www.example.org/SubscriptionManager
          </wsa:Address>
        </wsnt:SubscriptionReference>
        <wsnt:Topic Dialect=
"\"http://docs.oasis-open.org/wsn/t-1/TopicExpression/Simple\">
          npex:SomeTopic
        </wsnt:Topic>
        <wsnt:ConsumerReference>
          <wsa:Address>
            http://www.example.org/NotificationConsumer
          </wsa:Address>
        </wsnt:ConsumerReference>
        <wsnt:ProducerReference>
          <wsa:Address>
            http://www.example.org/NotificationProducer
          </wsa:Address>
        </wsnt:ProducerReference>
        <wsnt:Message>
          <npex:NotifyContent>exampleNotifyContent</npex:NotifyContent>
        </wsnt:Message>
      </wsnt:NotificationMessage>
    </wsnt:Notify>
  </s:Body>
</s:Envelope>

```

305

306

307 **Second proposal** (more general proposal, is based on the fact that WS-Notification is supported by WS-  
308 Addressing)

309 The WS-Addressing specification should be extended so that it expresses the concept of “final  
310 destination” of the message, by adding a new element, named for example <was:FinalTo>, in addition to  
311 those already present.

312

313 In this way the subscriber could specify both the NotificationProducer and the NotificationConsumer as  
314 final destinations in the subscription message.

```

<s:Envelope ... >
  <s:Header>
    <wsa:Action>
      http://docs.oasis-open.org/wsn/bw-
      2/NotificationProducer/SubscribeRequest
    </wsa:Action>
    <wsa:FinalTo>
      <wsa:Address> http://www.example.org/NotificationProducer
    </wsa:Address>
    </wsa:FinalTo>
    ...
  </s:Header>
  <s:Body>
    <wsnt:Subscribe>
      <wsnt:ConsumerReference>
        <wsa:FinalTo>
          <wsa:Address>
            http://www.example.org/NotificationConsumer
          </wsa:Address>
        </wsa:FinalTo>
      </wsnt:ConsumerReference>
      <wsnt:Filter>
        <wsnt:TopicExpression Dialect=
        "http://docs.oasis-open.org/wsn/t-1/TopicExpression/Simple">
          npex:SomeTopic
        </wsnt:TopicExpression>
        <wsnt:MessageContent
          Dialect="http://www.w3.org/TR/1999/REC-xpath-19991116">
          boolean(ncex:Producer="15")
        </wsnt:MessageContent>
      </wsnt:Filter>
      <wsnt:InitialTerminationTime>
        2005-12-25T00:00:00.000000Z
      </wsnt:InitialTerminationTime>
    </wsnt:Subscribe>
  </s:Body>
</s:Envelope>

```

316

317

318 The intermediary can send the message to the NotificationProducer without the necessity to make any  
 319 interpretation of the message.

320

321 As a consequence, the NotificationProducer knows the endpoints of the NotificationConsumer and of the  
 322 intermediary to which reply to; so it can send a notification to the intermediary, specifying the  
 323 NotificationConsumer as final destination.

324

```

<s:Envelope ... >
  <s:Header>
    <wsa:Action>
      http://docs.oasis-open.org/wsn/bw-2/NotificationConsumer/Notify
    </wsa:Action>
    <wsa:FinalTo>
      <wsa:Address> http://www.example.org/NotificationConsumer
    </wsa:Address>
    </wsa:FinalTo>
    ...
  </s:Header>
  <s:Body>
    <wsnt:Notify>
      <wsnt:NotificationMessage>
        <wsnt:SubscriptionReference>
          <wsa:Address>
            http://www.example.org/SubscriptionManager
          </wsa:Address>
        </wsnt:SubscriptionReference>
        <wsnt:Topic Dialect=
"\"http://docs.oasis-open.org/wsn/t-1/TopicExpression/Simple\"">
          npex:SomeTopic
        </wsnt:Topic>
        <wsnt:ProducerReference>
          <wsa:Address>
            http://www.example.org/NotificationProducer
          </wsa:Address>
        </wsnt:ProducerReference>
        <wsnt:Message>
          <npex:NotifyContent>exampleNotifyContent</npex:NotifyContent>
        </wsnt:Message>
        <wsnt:NotificationMessage>
      </wsnt:Notify>
    </s:Body>
  </s:Envelope>

```

325  
326

## 327 2.3 Requirements on SOAP

### 328 2.3.1 Identification of Use Case

329 Extract from [SOA-TEL 1.0], section 4.1 (rows 405 to 414):

330 -----

331 The perceived technical gap suggested is that the SOAP specification should be modified in order to  
332 enable a SOAP Intermediary node to “forward” the SOAP Header in automatic mode (thus without the

333 Header reinsertion) even if such node performs some processing operation over the body of the SOAP  
334 message.

335 Another way of expressing this perceived gap is to state that currently only 3 roles are allowed for a  
336 SOAP Node (i.e. initial SOAP Sender, SOAP intermediary, SOAP ultimate receiver – section 2.1 of the  
337 SOAP 1.2 specification), while a probable fourth role enabling the simultaneous body processing and  
338 header forwarding of a specific SOAP message may be needed.

339 -----

## 340 **2.3.2 Requirement(s)**

### 341 **Req. 3**

342 A new “Message Sender and Receiver concept” must be added in [SOAP 1.2] to model SOAP nodes  
343 which must forward the SOAP headers message, but also need to perform changes on the body of the  
344 message.

345 A new SOAP protocol must be added to manage the behavior of such nodes.

## 346 **2.3.3 Description**

347 As documented in the SOA-TEL TC “Use Cases and Issues” document, some SOAP nodes can’t be  
348 classified as “Ultimate SOAP Receivers” because they aren’t the real providers of the service, but can’t be  
349 simple “SOAP Intermediaries”, because they need to perform changes on the body of the message: such  
350 nodes aren’t requestors or receivers, they need to process the SOAP header blocks, perform some  
351 changes on the body, and forward the message to the following node.

352

353 Hereafter a proposal definition of the new “SOAP functional intermediary” (the name is provisional and  
354 could be different) concept is provided:

#### 355 • **SOAP functional intermediary**

356 - *A SOAP functional intermediary is both a SOAP receiver and a SOAP sender and is targetable from*  
357 *within a SOAP message. It processes the SOAP header blocks targeted at it and acts to forward a*  
358 *SOAP message towards an ultimate SOAP receiver. Moreover a SOAP Functional Intermediary*  
359 *can process the contents of the SOAP body.*

360

361 This new concept and its functionalities of both processing the body of a message and of forwarding  
362 headers as a usual “SOAP intermediary” are to be included in the SOAP specification.

## 363 **2.3.4 Solution proposals**

364 The following text is provided in order to illustrate some possible ways to address the Requirement. They  
365 are suggestions and are by no means to be considered as mandatory, as other possible options could be  
366 identified which are not represented hereafter.

367

368 To the best knowledge within OASIS SOA-TEL TC, the requirements presented hereafter could be  
369 addressed by the W3C “XML Protocol” Working Group, which produced the SOAP specification. Currently  
370 such group is in status “Completed”. For such reason, should the requirement be accepted, some  
371 preliminary investigations with W3C representatives are suggested to identify if within this SDO there are  
372 some WGs willing to consider and solve the issue.

373 Some modifications to [SOAP 1.2] are needed (but other parts of the specification may need to be revised  
374 and changed):

- 375 • Include the new concept definition in Section 1.5.3;
- 376 • Modify paragraphs 2.2 and 2.7 of [SOAP 1.2]. In particular, 2 cases are suggested.

377

378 **Case 1**

379 The SOAP functional intermediary typology is covered by the role “next”. In this case the SOAP  
 380 intermediary and SOAP functional intermediary act in a very similar way.

381 In this case Table 2 in section 2.2 should be modified as follows, while no changes should be required for  
 382 table 3 at section 2.7.1.

383

Table 2: SOAP Roles defined by this specification		
Short-name	Name	Description
next	"http://www.w3.org/2003/05/soap-envelope/role/next"	Each SOAP intermediary, <b>SOAP functional intermediary</b> , and the ultimate SOAP receiver <b>MUST</b> act in this role.
none	"http://www.w3.org/2003/05/soap-envelope/role/none"	SOAP nodes <b>MUST NOT</b> act in this role.
ultimateReceiver	"http://www.w3.org/2003/05/soap-envelope/role/ultimateReceiver"	The ultimate receiver <b>MUST</b> act in this role.

384

385 **Case 2**

386 The SOAP functional intermediary typology is covered by the role “ultimateReceiver”. In this case  
 387 Table 2 should be modified as follows:

388

Table 2: SOAP Roles defined by this specification		
Short-name	Name	Description
next	"http://www.w3.org/2003/05/soap-envelope/role/next"	Each SOAP intermediary, and the ultimate SOAP receiver <b>MUST</b> act in this role.
none	"http://www.w3.org/2003/05/soap-envelope/role/none"	SOAP nodes <b>MUST NOT</b> act in this role.
ultimateReceiver	"http://www.w3.org/2003/05/soap-envelope/role/ultimateReceiver"	The ultimate receiver and <b>SOAP functional intermediary</b> , <b>MUST</b> act in this role.

389

390 Moreover, table 3 in section 2.7.1 should be modified as follows:

391

Table 3: SOAP Nodes Forwarding behavior			
Role		Header block	
Short-name	Assumed	Understood & Processed	Forwarded
next	Yes	Yes	No, unless reinserted
		No	No, unless relay = "true"
user-defined	Yes	Yes	No, unless reinserted

		No	No, unless <code>relay = "true"</code>
	No	n/a	Yes
ultimateReceiver	Yes	Yes	No, unless <b>reinserted</b>
		No	No, unless <code>relay = "true"</code>
none	No	n/a	Yes

392

---

## 393 3 Requirements on Security

394

### 395 3.1 Requirements on Security Token Correlation

#### 396 3.1.1 Identification of Use Case

397 Currently it is not possible to correlate a security token with another one, previously created.

398 Refer section 5-1 of [SOA-TEL 1.0], in which the technical issue is documented.

#### 399 3.1.2 Requirement(s)

##### 400 Req. 4

401 The WS Security specifications must enable to express a relation between two security tokens, a “main”  
402 token (e.g. named “*token2*”) and a “related” token (e.g. named “*token1*”).

403 The characteristics of the relation are that, when the token correlation is used,

- 404 • the “main” token can not be built without being in possession of the “related” token,
- 405 • the WS-Sec header should not be considered valid if the “related” token is not present.

406 This token correlation requirement defines a new token security model, in which a “main” token is  
407 syntactically and semantically meaningful if it is built and presented in relation with another “related”  
408 token.

##### 409 SOA-TEL Req. 4.1

410 It must be possible to express “token correlation” also into the SAML assertion.

#### 411 3.1.3 Description

412 This token correlation requirement extends the message security models and enforces the security  
413 mechanism in environments where the message exchange pattern is more complex than the simple  
414 “requestor – provider” pattern.

415 This model should be useful when the definition and the use of a “simple” token doesn’t guarantee a  
416 sufficient level of security, since the authorization to access a specific service also depends on the fact  
417 that a previous token was released.

418

419 The possible “status” of the “related” token could be valid or expired (i.e. not valid anymore).

420 In the new token typology to be introduced, the “related” token is not a simple “attribute”, inserted only for  
421 traceability purposes into the header, but instead is an integral part of the token.

422 The identity provider should release the security token directly made up of two parts: the “main” and the  
423 “related” tokens.

#### 424 3.1.4 Solution proposals

425 The following text is provided in order to illustrate some possible ways to address the Requirement. They  
426 are suggestions and are by no means to be considered as mandatory, as other possible options could be  
427 identified which are not represented hereafter.

428 [WS-S 1.1] defines three types of security tokens and how they are attached to messages (“user name  
429 token”, “binary security token” and “XML token”), and furthermore the syntax provides 2 elements to  
430 include tokens in the security header:



- 431 • <wsse:UsernameToken>
- 432 • <wsse:BinarySecurityToken>.

433

434 A new element should be added, named for example <wsse:AssociatedToken> to the previous ones.

435 The <wsse: AssociatedToken> could contain (in a recursive manner) a username token, or a binary

436 token, or a XML token element, or again a related token, for the “main” token.

437 The same should be for the “related” token.

438

439 This could be the syntax of the element:

440

```

441 <wsse: AssociatedToken>
442     <wsse:MainToken>
443         .....
444     </wsse: MainToken>
445     <wsse:RelatedToken>
446         .....
447     </wsse:RelatedToken>
448 </wsse:AssociatedToken>

```

449

450 This is an example of associated token:

451

```

<?xml version="1.0" encoding="utf-8"?>
<S11:Envelope xmlns:S11="..." xmlns:wsse="..." xmlns:wsu="..." xmlns:ds="...">
<S11:Header>
  <wsse:Security xmlns:wsse="...">
    <wsse:AssociatedToken Value Type wsu:Id=" MyNewT">
      <wsse:MainToken>
        <wsse:UsernameToken wsu:Id="MyMainT">
          <wsse:Username>...</wsse:Username>
        </wsse:UsernameToken>
      </wsse:MainToken>
    <wsse:RelatedToken>
      <wsse:BinarySecurityToken Value Type=" http://fabrikam123#CustomToken "
        EncodingType="...#Base64Binary" wsu:Id=" MyID ">
        FHUIORv...
      </wsse:BinarySecurityToken>
    </wsse:RelatedToken>
  </wsse:Security>
</S11:Header>
</S11:Envelope>

```

452

453

454 The <wsse:AssociatedToken> element could have other significant elements (other than the related

455 token value) useful to the definition of the context in which the main token was built; for example it could

456 include the timestamp value present in the security header from which the related token derive. Examples

457 of other significant elements may also be (but not limited to) the ones currently defined within the three

458 above mentioned security tokens types.

460 In other words if the related security token belonged to the following header:

461

```
462 <S11:Header>
463   <wsse:Security>
464     <wsu:Timestamp wsu:Id="T0">
465       <wsu:Created>
466         2001-09-13T08:42:00Z</wsu:Created>
467     </wsu:Timestamp>
468
469   <wsse:BinarySecurityToken
470     ValueType="...#X509v3"
471     wsu:Id="X509Token"
472     EncodingType="...#Base64Binary">
473     MIEZzCCA9CgAwIBAgIQEmtJZc0rqrKh5i...
474   </wsse:BinarySecurityToken>
```

475

476 The AssociatedToken in the new header should be the following:

477

```
<?xml version="1.0" encoding="utf-8"?>
<S11:Envelope xmlns:S11="..." xmlns:wsse="..." xmlns:wsu="..." xmlns:ds="...">
<S11:Header>
  <wsse:Security xmlns:wsse="...">
    <wsse:AssociatedToken ValueType wsu:Id=" MyNewT">
      <wsse:MainToken>
        <wsse:UsernameToken wsu:Id="MyMainT">
          <wsse:Username>...</wsse:Username>
        </wsse:UsernameToken>
      </ wsse:MainToken>
      <wsse:RelatedToken>
        <wsu:Timestamp wsu:Id="T0">
          <wsu:Created>
            2001-09-13T08:42:00Z</wsu:Created>
          </wsu:Timestamp>
        <wsse:BinarySecurityToken
```

478

479

480 Clearly this mechanism is particularly meaningful when the related token is a SAML assertion that  
481 supplies all the information to describe the context in which the main token was built, that is the objective  
482 of the requirement.

483 In a similar way the SAML protocol could be extended to support the requirement.

484 In this case a new AssociatedToken element could be added into the SAML syntax, so the related token  
485 could be included directly in the SAML assertion constituting the main token, without the necessity of  
486 express the relation to the WS security header level.

487

488 **3.2 SAML Name Identifier Request**

489 **3.2.1 Identification of Use Case**

490 A user device, a Service Provider (SP) and an Identity Provider (IdP) are the actors of this use case. The  
491 SP is new to the circle of trust of the IdP. The IdP does not know a name identifier of the user device. The  
492 IdP requests a name identifier from the SP, who sends the desired name identifier to the IdP.

493 Section 5.2.2 in [SOA-TEL 1.0] describes a use case for the proposed SAML Name Identifier Request-  
494 Response protocol.

495 **3.2.2 Requirement(s)**

496 **Req. 5**

497 In order to make the [SAML 2.0] support name identifier use cases such as that described in section  
498 3.2.1, the Security Services TC must specify a

- 499 • <NameIdentifierRequest> message sent from an Identity Provider to a Service Provider to request a  
500 name identifier for a User, and a
- 501 • <NameIdentifierResponse> message sent from the Service Provider to the Identity Provider to return  
502 such a name identifier to the Identity Provider.

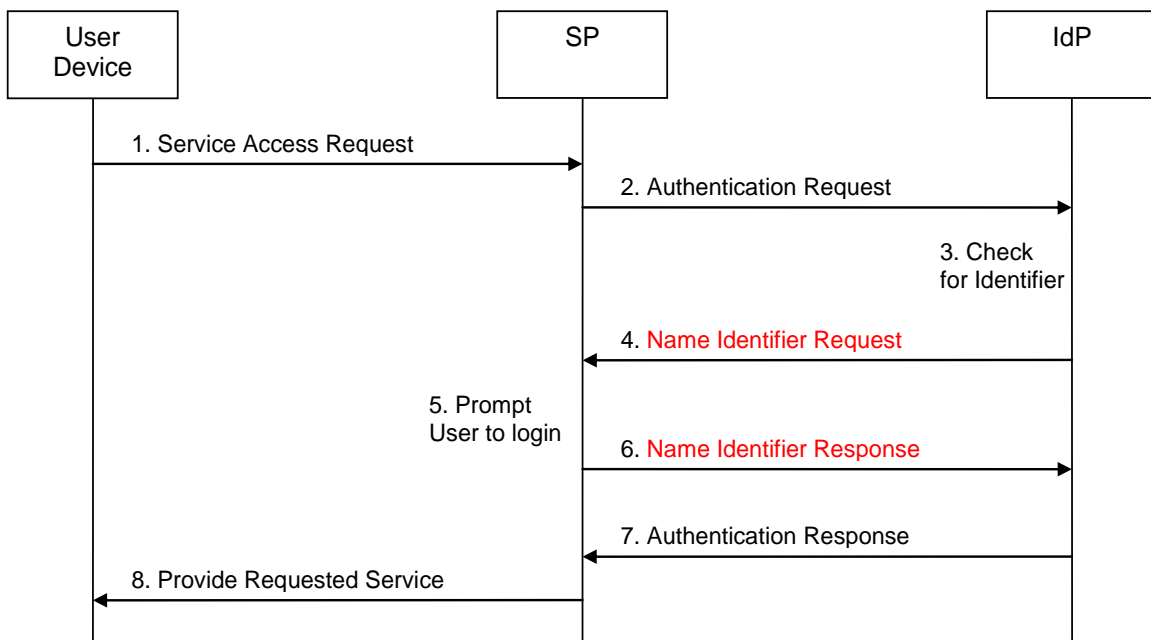
503 This requires extensions to the existing [SAML 2.0] core specification (saml-core-2.0-os) including the  
504 SAML 2.0 protocol schema. No modification of the existing SAML 2.0 assertion schema is necessary.

505 Description

506 [Figure 4](#)

507 [Figure 4](#) provides a high-level message flow illustrating the proposed SAML Name Identifier request-  
508 response protocol. Messages 4 and 6 belong to the proposed SAML Name Identifier Request protocol.  
509 These messages are interlaced into the SAML Authentication Request and Response exchange between  
510 SP and IdP and are not specified in SAML V2.0 yet (therefore, marked in red):

511



512

513

514 Figure 4: SAML Name Identifier request-response use case: pictorial representation

515

516 The single steps of this use case are as follows:

517

- 518 1) The user requests access to a service offered by a SP. The user device does not include any  
519 authentication credentials.
- 520 2) Since access to this service requires the User to be authenticated but the request in step 1 does not  
521 include any authentication credentials, the SP sends an Authentication Request to the IdP. This  
522 Authentication Request may be passed to the IdP via the user device using redirection.
- 523 3) The IdP checks the Authentication Request received in step 2, and - as the SP is new to the IdP's  
524 circle of trust - the IdP determines that it does not have an identifier stored in its database for the User  
525 for the given SP.
- 526 4) This step is not defined in SAML V2.0: Since the IdP has realized in step 3 that it does not have an  
527 identifier for the combination of the User and the SP, the IdP generates a message called Name  
528 Identifier Request and sends it to the SP.
- 529 5) Upon receipt of the Name Identifier Request, the SP recognises that the IdP does not have an  
530 identifier for the combination of SP and User. Therefore, the SP prompts the User to log in to the SP.
- 531 6) This step is also not defined in SAML V2.0: The SP sends a message called Name Identifier  
532 Response to the IdP. This response message includes the identifier for the combination of User and  
533 SP that the IdP is to use in any further communication and authentication processes.
- 534 7) On receipt of the Name Identifier Response, the IdP stores the identifier contained in the Name  
535 Identifier Response in its database. The IdP sends an Authentication Response to the SP, which  
536 uses the identifier received in step 6.
- 537 8) The SP grants the User access to the requested service.

538

539 In step 3 of the message exchange illustrating a SAML Name Identifier use case above, conventionally,  
540 the IdP would respond to the Authentication Request (step 2) by issuing an error message or a randomly  
541 generated identifier. This, however, is problematic: In the former case, the service access request in step  
542 1 breaks down. In the latter case, the SP has to ask the user for his credentials and then send (usually via  
543 a backchannel) a message to the IdP indicating that from now on the IdP should use the "real identifier"  
544 instead of the random one for the given user (this could be done via the NameIdentifier Management  
545 Protocol).

546 These issues can be resolved on SAML protocol level by defining <NameIdentifierRequest> and  
547 <NameIdentifierResponse> messages enabling the Identity Provider to request from a Service Provider a  
548 name identifier for a User and the Service Provider to send such a name identifier back to the Identity  
549 Provider.

### 550 3.2.3 Solution proposal

551 Extension of the SAML 2.0 protocol schema by <NameIdentifierRequest> and  
552 <NameIdentifierResponse> messages, instances of which are exemplified as follows:

553

554 *Name Identifier Request:*

555

```
556 <samlp:NameIdentifierRequest
557     xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
558     xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
559     ID="aaf23196-1773-2113-474a-fe114412ab72"
560     Version="2.0"
561     IssueInstant="2006-07-17T20:31:40Z">
562     <saml:Issuer
```

```

563         Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">
564         http://idm.nsn.com
565     </saml:Issuer>
566 </samlp:NameIdentifierRequest>
567
568 Name Identifier Response:
569
570 <samlp:NameIdentifierResponse
571     xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
572     xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
573     ID="aaf23196-1773-2113-474a-fe114412ab72"
574     Version="2.0"
575     IssueInstant="2006-07-17T20:31:40Z">
576
577     <saml:Assertion
578         MajorVersion="1" MinorVersion="0"
579         AssertionID="128.9.167.32.12345678"
580         Issuer="Smith Corporation">
581         <saml:Issuer
582             Format="urn:oasis:names:tc:SAML:1.1:nameid-
583             format:X509SubjectName">
584             C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
585         </saml:Issuer>
586         <saml:Subject>
587             <saml:NameID
588                 Format="urn:oasis:names:tc:SAML:1.1:nameid-
589                 format:unspecified">
590                 tom.smith
591             </saml:NameID>
592         </saml:Subject>
593
594         <saml:AttributeStatement>
595             <saml:Attribute
596                 xmlns:x500="urn:oasis:names:tc:SAML:2.0:
597                 profiles:attribute:X500"
598                 x500:Encoding="LDAP"
599                 NameFormat="urn:oasis:names:tc:SAML:2.0:
600                 attrname-format:uri"
601                 Name="urn:oid:2.5.4.42"
602                 FriendlyName="givenName">
603                 <saml:AttributeValue xsi:type="xs:string">
604                     Tom
605                 </saml:AttributeValue>
606             </saml:Attribute>
607
608             <saml:Attribute

```

```

609         xmlns:x500="urn:oasis:names:tc:SAML:2.0:
610         profiles:attribute:X500"
611         x500:Encoding="LDAP"
612         NameFormat="urn:oasis:names:tc:SAML:2.0:
613         attrname-format:uri"
614         Name="urn:oid:1.3.6.1.4.1.1466.115.121.1.26"
615         FriendlyName="mail">
616         <saml:AttributeValue xsi:type="xs:string">
617             trscavo@gmail.com
618         </saml:AttributeValue>
619     </saml:Attribute>
620 </saml:AttributeStatement>
621 </saml:Assertion>
622 <samlp:Status xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
623     <samlp:StatusCode
624         xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
625         Value="urn:oasis:names:tc:SAML:2.0:status:Success">
626     </samlp:StatusCode>
627 </samlp:Status>
628 </samlp:NameIdentifierResponse>
629

```

## 630 3.3 SAML Attribute Management Request

### 631 3.3.1 Identification of Use Case

632 A user wishes to use his attribute information across multiple service providers. Such attribute information  
633 can be layout, preferred email address, etc. Today, these attributes are stored locally at each service  
634 provider. Thus, the user will have to enter and change the same attributes multiple times in order to  
635 ensure they are consistent for each of the different service providers the user has an account with,  
636 resulting in a bad user experience.

637 The user creates a temporary or transient account. The service provider allows the user to set specific  
638 settings like coloring, text size, etc. But he/she does not want to set these setting again each time the  
639 user logs in because the service provider will not be able to link the attributes for a user's temporary  
640 account with the user's permanent account. This is because by the very nature of a temporary or  
641 transient account the next time the user logs on to the service provider the user will have a different user  
642 name and so the service provider will not be able to link the attributes for a user's temporary account with  
643 the user's permanent account.

644 Section 5.3.2 in [SOA-TEL 1.0] describes a use case for the proposed SAML Attribute Management  
645 Request-Response protocol.

646

### 647 3.3.2 Requirement(s)

#### 648 Req. 6

649 In order to make the [SAML 2.0] support attribute management use cases such as that described in 3.3.1,  
650 the Security Services TC must specify a

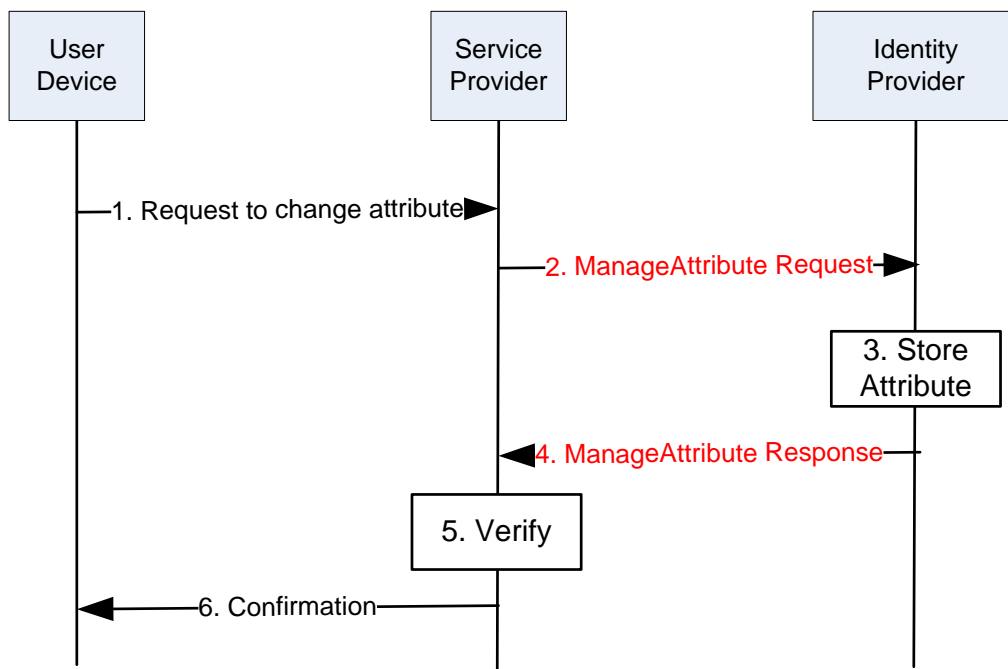
- 651 • <ManageAttributeRequest> message sent from a Service Provider to an Identity Provider to request  
652 a modification or the storage of an attribute, and a

653 • <ManageAttributeResponse> message sent from the Identity Provider to the Service Provider to  
654 return to the Service Provider the result of processing the received <ManageAttributeRequest>  
655 message.

656 This requires extensions to the existing SAML 2.0 core specification (saml-core-2.0-os) including the  
657 SAML 2.0 protocol schema. No modification of the existing SAML 2.0 assertion schema is necessary.  
658

### 659 3.3.3 Description

660 Figure 5 provides a high-level message flow outlining the proposed SAML Attribute Management  
661 protocol:



662  
663 Figure 5: SAML Attribute Management request-response use case: pictorial representation  
664

665 The Manage Attribute Request and Response messages are marked in red since the SAML 2.0 does not  
666 support such messages yet. The ManageAttribute Request allows the Service Provider to manage  
667 attributes stored on the Identity Provider side.

### 668 3.3.4 Solution proposal

669 Extension of the SAML 2.0 protocol schema by <ManageAttributeRequest> and  
670 <ManageAttributeResponse> messages, instances of which are exemplified as follows:

671  
672 *Manage Attribute Request:*  
673

```
674 <samlp:ManageAttributeRequest
675     xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
676     xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
677     ID="aaf23196-1773-2113-474a-fe114412ab72"
```

```

678     Version="2.0"
679     IssueInstant="2006-07-17T20:31:40Z">
680     <saml:Issuer
681         Format="urn:oasis:names:tc:SAML:1.1:nameidformat:
682         X509SubjectName">
683         C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
684     </saml:Issuer>
685
686     <saml:Subject>
687         <saml:NameID
688             Format="urn:oasis:names:tc:SAML:1.1:nameidformat:X50
689             SubjectName">
690             C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
691         </saml:NameID>
692     </saml:Subject>
693     <saml:AttributeStatement>
694         <saml:Attribute
695             xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:
696             attribute:X5 00" x500:Encoding="LDAP"
697             NameFormat="urn:oasis:names:tc:SAML:2.0:
698             attrname-format:uri"
699             Name="urn:oid:2.5.4.42"
700             FriendlyName="givenName">
701             <saml:AttributeValue
702                 xsi:type="xs:string">
703                 John
704             </saml:AttributeValue>
705         </saml:Attribute>
706         <saml:Attribute
707             xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:
708             attribute:X500" x500:Encoding="LDAP"
709             NameFormat="urn:oasis:names:tc:SAML:2.0:
710             attrname-format:uri"
711             Name="urn:oid:1.3.6.1.4.1.1466.115.121.1.26"
712             FriendlyName="mail">
713             <saml:AttributeValue
714                 xsi:type="xs:string">
715                 johndoe@gmail.com
716             </saml:AttributeValue>
717         </saml:Attribute>
718     </saml:AttributeStatement>
719 </samlp:ManageAttributeRequest>
720

```



721

722 *Manage Attribute Response:*

723

724 <samlp:ManageAttributeResponse

725     xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"

726     xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"

727     ID="aaf23196-1773-2113-474a-fe114412ab72"

728     Version="2.0"

729     IssueInstant="2006-07-17T20:31:40Z">

730     <saml:Assertion

731         MajorVersion="1" MinorVersion="0"

732         AssertionID="128.9.167.32.12345678"

733         Issuer="Smith Corporation">

734         <saml:Issuer

735             Format="urn:oasis:names:tc:SAML:1.1:

736             nameid-format:unspecified">

737             http://idm.nsn.com

738         </saml:Issuer>

739         <saml:Subject>

740             <saml:NameID

741                 Format="urn:oasis:names:tc:SAML:1.1:

742                 nameid10format:X509SubjectName">

743                 C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu

744             </saml:NameID>

745         </saml:Subject>

746         <saml:AttributeStatement>

747             <saml:Attribute

748                 xmlns:x500="urn:oasis:names:tc:SAML:2.0:

749                 profiles:attribute:X500"

750                 x500:Encoding="LDAP"

751                 NameFormat="urn:oasis:names:tc:SAML:2.0:

752                 attrname-format:uri"

753                 Name="urn:oid:2.5.4.42"

754                 FriendlyName="givenName">

755                 <saml:AttributeValue

756                     xsi:type="xs:string">

757                     John

758                 </saml:AttributeValue>

759             </saml:Attribute>

760             <saml:Attribute

761                 xmlns:x500="urn:oasis:names:tc:SAML:2.0:

762                 profiles:attribute:X500"

763                 x500:Encoding="LDAP"

```
764         NameFormat="urn:oasis:names:tc:SAML:2.0:
765         attrname-format:uri"
766         Name="urn:oid:1.3.6.1.4.1.1466.115.121.1.26"
767         FriendlyName="mail">
768         <saml:AttributeValue
769             xsi:type="xs:string">
770             trscavo@gmail.com
771         </saml:AttributeValue>
772     </saml:Attribute>
773 </saml:AttributeStatement>
774 </saml:Assertion>
775 <samlp:Status
776     xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
777     <samlp:StatusCode
778         xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
779         Value="urn:oasis:names:tc:SAML:2.0:status:Success">
780     </samlp:StatusCode>
781 </samlp:Status>
782 </samlp:ManageAttributeResponse>
```

## 783 3.4 User ID Forwarding

### 784 3.4.1 Scenario/context

### 785 3.4.2 Identification of Use Case

786 Currently a standard way does not exist to add two (or more) credentials in one message.  
787 Refer to section 5-4 of [SOA-TEL 1.0], in which the technical issue is documented.

### 788 3.4.3 Requirement(s)

#### 789 Req. 7

790 The WS Security specifications must enable to bring two security credentials in the security header: the  
791 “main” credential (e.g. named “*credential2*”) and a “secondary” credential (e.g. named “*credential1*”).  
792 The authentication and authorization process should be performed on the basis of the main credential;  
793 the secondary credential should be used to complete the security functionalities.

#### 794 [SOA-TEL Req. 7.1]

795 It must be possible to express support two credentials also into the SAML assertion.  
796

### 797 3.4.4 Description

798 The user-id forwarding requirement extends the message security models and enforces the security  
799 mechanism in environments where a second security credential is necessary to add functionalities to the  
800 basic security process.

801 This model should be useful when the process of authentication and authorization on the base of the  
802 credential provided in the security header is not enough, and other security functionalities have to be  
803 executed on a second credential, for example to complete the authorization process or to profile the data.

### 804 3.4.5 Solution proposals

805 The following text is provided in order to illustrate some possible ways to address the Requirement. They  
806 are suggestions and are by no means to be considered as mandatory, as other possible options could be  
807 identified which are not represented hereafter.

808

809 To the best knowledge within OASIS SOA-TEL TC, the requirements presented hereafter could be  
810 addressed by the OASIS Web Services Security (WSS) TC, which by the way is in status "Completed",  
811 and possibly by the OASIS Security Services (SAML) TC.

812

813 Hereafter some suggestions are proposed.

814 The WS-Sec v1.1 specification defines the following elements:

```
815 /wsse:Security;  
816 /wsse:Security/@S11:actor;  
817 /wsse:Security/@S12:role;  
818 /wsse:Security/@S11:mustUnderstand;  
819 /wsse:Security/{any};  
820 /wsse:Security/ @{any};
```

821

822 Another element should be added, named for example:

823 /wsse:SecondaryCredential. This element should contain a security token, in particular one of the tokens  
824 provided by the current WS Security specification.

825

826 This is an example of header with a secondary credential, when the main credential is represented by a  
827 binary token, and the secondary by a user name and password token:

828

```
<?xml version="1.0" encoding="utf-8"?>  
<S11:Envelope xmlns:S11="..." xmlns:wsse="..." xmlns:wsu="..." xmlns:ds="...">  
<S11:Header>  
  <wsse:Security xmlns:wsse="...">  
    <wsse:BinarySecurityToken ValueType=" http://fabrikam123#CustomToken "  
      EncodingType="...#Base64Binary" wsu:Id=" MyID ">  
      FHUIORv...  
    </wsse:BinarySecurityToken>  
    <wsse:SecondaryCredential ValueType wsu:Id=" MyNewT">  
      <wsse:UsernameToken wsu:Id="MyMainT">  
        <wsse:Username>...</wsse:Username>  
      </wsse:UsernameToken>  
    </wsse:SecondaryCredential>  
  </wsse:Security>  
</S11:Header>  
.....
```

829

830

831

832 In a similar way the SAML protocol could be extended to support the requirement.

833 In this case the “secondary credential” element could be added into the SAML syntax. In this way the  
834 related token could be included directly in the SAML assertion which constitutes the main token, without  
835 the necessity of express the relation to the WS security header level.

836

837 As an alternative path, the following hypothesis can be considered. This requirement (User-id forwarding  
838 requirement) is “intrinsically” similar to the “Security token correlation” requirement, presented elsewhere  
839 in the present document. Thus a common approach in modifying the WS-Security specifications could be  
840 adopted to address both the requirements and, more in general, similar security issues.

---

## 841 4 Requirements on Management

### 842 4.1 Cardinality of a Service Interface

#### 843 4.1.1 Identification of Use Case

844 Extract from [SOA-TEL 1.0], section 6.3:

845 -----

846 [SOA-RM 1.0]: (Section 3.1) “A service is accessed by means of a service interface (see Section  
847 3.3.1.4), where the interface comprises the specifics of how to access the underlying capabilities.”

848 [SOA-RM 1.0]: (Subsection 3.3.1.4) “**The** service interface is the means for interacting with a service.”

849 [SCA Assembly 1.1]: “A Service represents **an** addressable interface of the implementation.”

850 Note – SCA definition for Service may be a consequence of the SOA-RM definition, we do not know

851 -----

852 -----

853 [SOA-RA 1.0] (3137 – 3140) “In fact, managing a service has quite a few similarities to using a  
854 service: suggesting that we can use the service oriented model to manage SOA-based systems as  
855 well as provide them. A management service would be distinguished from a non-management service  
856 more by the nature of the capabilities involved (i.e., capabilities that relate to managing services) than  
857 by any intrinsic difference. “

858 -----

#### 859 4.1.2 Requirement(s)

##### 860 Req. 8

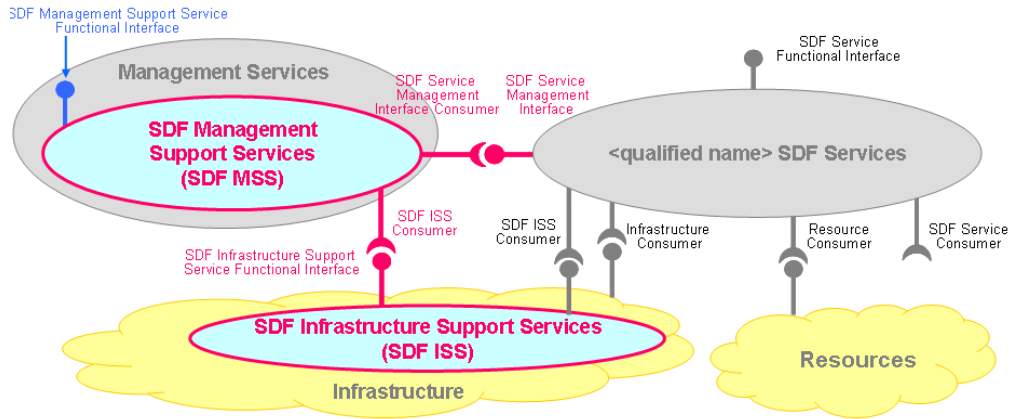
861 The SOA Reference Model and Architecture must explain how a service separates and exposes its  
862 manageability capabilities to allow other services to manage it.

863 The Service Delivery Framework specified by TM Forum and depicted below sets such requirement at the  
864 SDF Service Management Interface (indicated in red in

865 [Figure 6](#)

866 [Figure-6](#)).

867



868  
869  
870

Figure 6: TM Forum SDF Reference Model

871 **4.1.3 Description**

872 As documented in the SOA-TEL TC “Use Cases and Issues”, interfaces are the ways to interact with and  
873 between services and interfaces are the way to expose capabilities. At the same time, TM Forum SDF  
874 requires that SDF Services expose both Functional and Management capabilities and recommends this  
875 exposure to be made at separate interfaces attached to the SDF Service.

876 **4.1.4 Solution proposals**

877 OASIS SCA Assembly Model specification v1.1 offers a solution to the multiple interfaces problem as well  
878 as to “marking” an interface as being a management interface.

879 Updates to this specification (Committee Draft 03 rev 1.1 June 2009) offer also support for dynamic wiring  
880 of “service references” with “services” at run time through “autowire”, policy sets and SCA runtime re-  
881 evaluation of targets.

882 These proposals will be tested through TM Forum’s use case analysis and the results will be sent back to  
883 OASIS SCA Assembly team for further discussion.

884

885 Observations:

- 886 1. SCA Assembly Model covers only design, deployment and runtime as manageable capabilities (or  
887 management operations) for software bundles that constitute SDF Services. Other aspects of service  
888 lifecycle management such as quality, charging are not part of OASIS charter and will be further  
889 investigated by TM Forum in collaboration with other industry organizations.
- 890 2. SCA Assembly Model is not yet mapped to the OASIS SOA RA/RM.

891 **4.2 Requirements on Metadata**

892 **4.2.1 Identification of Use Case**

893 Extract from [SOA-TEL 1.0], section 6-4:

894 -----

895 Specialization in supporting and managing a service during its whole lifecycle requires finer granularity  
896 knowledge about that service: properties, supported actions or operations, possible states as well as  
897 contracts that may govern interactions with the service (including pre and post conditions for these  
898 interactions), what is the “architectural” style for service “composability”, what are its dependencies or  
899 what is the level of exposure for its functional capabilities.

900 The proposed model for the TMF SDF Service is complemented by additional data representation  
901 (metadata) in support of SDF Service lifecycle management (ref. Section 6.4 – [SOA-TEL 1.0]). This new  
902 data representation containing information about the service in various phases of its lifecycle, aims at  
903 covering current gaps in the information available for the purpose of service management (e.g. what is  
904 already covered by the SOA Service description) in the overall context of Service Provider's business and  
905 operations. Moreover, this metadata is dynamic: it may change from one phase to another of the SDF  
906 Service lifecycle.

907

908 The SDF Service Lifecycle Metadata consists at least of:

- 909 1. Additional information about the SMI of a SDF Service (properties, actions);
- 910 2. Management Dependencies of the SDF Service, including cross-domains dependencies;
- 911 3. Management State of the SDF Service.

912 -----

## 913 **4.2.2 Requirement(s)**

### 914 **Req. 9**

915 A standardization body (most probable TM Forum) must normalize the meta-data of Service Management  
916 to address the needs of managing any service from a lifecycle perspective. The meta-data should evolve  
917 into a meta-model that can be automatically instantiated into current and future management models  
918 which are domain (network or IT), technology (enterprise Java, IP network) or lifecycle phase (service  
919 creation, deployment, operation, etc).

### 920 **4.2.3 Description**

921 As documented in the SOA-TEL TC "Use Cases and Issues", paragraph 6.4, managing a service through  
922 its entire lifecycle requires finer granularity information (about the service, its execution environment, its  
923 dependencies, etc) than it is available today through management applications and tools. Moreover, this  
924 information, even when it is available (and most of it already exists) it comes in "bits and pieces", usually  
925 uncorrelated, from many places (tools, interfaces, environments) following diverse data models (SID,  
926 CIM, etc).

927 TM Forum SDF initiative believes that completing and unifying service management information through a  
928 well defined meta-data that describes and evolves with the lifecycle of each service instance is key to  
929 solving the issue of rapid service creation and launch.

930 The real problem to address is management across domains; the existence of different standards for  
931 metadata is an obstacle to the achievement of such objective.

### 932 **4.2.4 Solution proposals**

933 TM Forum SDF initiative started to define elements of service lifecycle management meta-data and show  
934 how they can be used in a service oriented management framework such as SDF (see fig 23 in OASIS  
935 UC document).

936 Nevertheless, TM Forum is not a data modeling or IT standards organization hence it raises the call to  
937 contributions to such organizations through OASIS SOA-Tel in the following areas:

- 938 - Representation of actions or state machines into meta-data (maybe OMG – UML 2.x)
- 939 - Support of versioning and compatibility of this meta-data
- 940 - Support of cohesiveness across metadata elements when they are updated from different  
941 sources and along the phases in the lifecycle of a service.
- 942 - Best design patterns for building and maintaining a repository for this meta-data

943 Today there is no clarity as to where to find such standards or if they exist and if they do not exist which  
944 organization should take the responsibility of working on them

---

## 945 5 Requirements on SOA collective standards usage

### 946 5.1 Common Patterns for Interoperable Service Based 947 Communications

#### 948 5.1.1 Identification of Use Case

949 This section is related to the specification of requirements related to the perceived technical issues  
950 identified in section 7, [SOA-TEL 1.0].

#### 951 5.1.2 Requirement(s)

##### 952 Req. 10

953 A common communications profile should be defined such that all multi tier web/ mobile applications  
954 declaring support for the profile will be able to establish a converged sessions irrespective of the  
955 underlying protocols, network domains and access across one or more servers/ services within or across  
956 different respective domains.

957 Such a profile will need to define an agreed to approach to:

- 958 1. Establish a session id for the context of converged application.
- 959 2. Ability to set up event sync supporting a common set of set of bi-directional event classes (i.e.  
960 push, broadcast, pub/sub, etc.).
- 961 3. Universally agreed to means to access the meta-data to discover the interface, binding, events  
962 classes, capability of service and device.
- 963 4. Common and agreed upon means/ nomenclature for an application in real-time to discover,  
964 advertise and negotiate device characteristics, codec's and communication modes with a peer or  
965 set of peers.
  - 966 o Device attributes, communication protocols and media negotiation achieved through two  
967 way services interaction.
  - 968 o This interaction can default to common underlying negotiation means if available/  
969 discoverable at setup time.

#### 970 5.1.3 Description

971 The Internet has been enormously successful as an environment allowing user centric viral application  
972 growth. Its success, among other things, is the result of passing control to the end user and abstracting  
973 the underlying network details out of the picture for the application. As the name denotes, The Internet  
974 was designed to allow networks to interoperate. Unfortunately, communication oriented application  
975 models are more often bound to specific network domains with dependencies across different underlying  
976 VoIP protocols, competing standards, discovery data models and session negotiation and establishment.

977 There are a growing set of application models that serve a general web and mobile market that can not  
978 "build-in" assumptions of the underlying network or multi-modal connection establishment. The  
979 communication profile is an attempt to mitigate this problem. It does not seek to enforce one standard  
980 over the other but attempts to establish a general framework allowing converged applications to  
981 interoperate thru normalized patterns of session establishment and discovery.



982

## 6 Conformance

983 The objective of this document is to collect requirements to address technical issues and gaps of SOA  
984 standards (specified by OASIS and other SDOs) utilized within the context of Telecoms. Such issues are  
985 documented in SOA-TEL's TC first deliverable "Telecom Use Cases and Issues, v.1.0".

986 For each requirement listed in this document, a specific conformance rule applies. In the following are  
987 listed

988

### 989 **Conformance to Requirement 1**

990 A future version of WS Addressing specification must include additional fields (in addition to the ones  
991 already present) containing remote destinations to which reply messages must be sent.

992

### 993 **Conformance to Requirement 2**

994 A future version of WS-Notification specification must provide a mechanism to describe and regulate a  
995 scenario in which one or more intermediaries are present.

996

### 997 **Conformance to Requirement 3**

998 A future version of SOAP specifications must include a new "Message Sender and Receiver concept" to  
999 model SOAP nodes which must forward the SOAP headers message, but also need to perform changes  
1000 on the body of the message

1001

### 1002 **Conformance to Requirement 4**

1003 A future version of WS Security specifications must enable to express a relation between two security  
1004 tokens, a "main" token (e.g. named "*token2*") and a "related" token (e.g. named "*token1*").

1005

### 1006 **Conformance to Requirement 4.1**

1007 In a future version of the SAML Specification (or a new profile of this specification ) it must be possible to  
1008 express "token correlation" into the SAML assertion.

1009

### 1010 **Conformance to Requirement 5**

1011 The SAML 2.0 protocol must support name identifier use cases by means of

- 1012 • <NameIdentifierRequest> message sent from an Identity Provider to a Service Provider to request a  
1013 name identifier for a User, and a
- 1014 • <NameIdentifierResponse> message sent from the Service Provider to the Identity Provider to return  
1015 such a name identifier to the Identity Provider.

1016 .

### 1017 **Conformance to Requirement 6**

1018 The SAML 2.0 protocol must support attribute management use cases by means of

- 1019 • <ManageAttributeRequest> message sent from a Service Provider to an Identity Provider to request  
1020 a modification or the storage of an attribute, and a
- 1021 • <ManageAttributeResponse> message sent from the Identity Provider to the Service Provider to  
1022 return to the Service Provider the result of processing the received <ManageAttributeRequest>  
1023 message.

1024

### 1025 **Conformance to Requirement 7**

1026 A future version of WS Security specifications must enable to bring two security credentials in the security  
1027 header: the “main” credential (e.g. named “*credential2*”) and a “secondary” credential (e.g. named  
1028 “*credential1*”) so that the authentication and authorization process could be performed on the basis of the  
1029 main credential, while the secondary credential could be used to complete the security functionalities.

1030

1031 **Conformance to Requirement 7.1**

1032 In a future version of the SAML Specification (or a new profile of this specification) it must be possible to  
1033 support two credentials into the SAML assertion.

1034

1035 **Conformance to Requirement 8**

1036 A future version of the OASIS SOA Reference Model and Architecture must explain how a service  
1037 separates and exposes its manageability capabilities to allow other services to manage it.

1038

1039 **Conformance to Requirement 9**

1040 A standardization body (most probable TM Forum) must have normalized the meta-data of Service  
1041 Management to address the needs of managing any service from a lifecycle perspective.

1042

1043 **Conformance to Requirement 10**

1044 A common communications profile should have been defined such that all multi tier web/ mobile  
1045 applications declaring support for the profile will be able to establish a converged sessions irrespective of  
1046 the underlying protocols, network domains and access across one or more servers/ services within or  
1047 across different respective domains.

---

1048 **Appendix A. Acknowledgements**

1049 The following individuals have participated in the creation of this specification and are gratefully  
1050 acknowledged:

1051

1052 **Participants:**

1053		
1054	Mike Giordano	Individual
1055	Ian Jones	BT
1056	Paul Knight	Individual
1057	Lucia Gradinariu	LGG Solutions
1058	Orit Levin	Microsoft
1059	Joerg.Abendroth	Nokia Siemens Networks
1060	Christian Guenter	Nokia Siemens Networks
1061	Thinn Nguyenphu	Nokia Siemens Networks
1062	Olaf Renner	Nokia Siemens Networks
1063	Abbie Barbir	Individual
1064	Vincenzo Amorino	Telecom Italia
1065	Luca Galeani	Telecom Italia
1066	Maria Jose Mollo	Telecom Italia
1067	Enrico Ronco	Telecom Italia
1068	Federico Rossini	Telecom Italia
1069	Luca Viale	Telecom Italia

## Appendix B. SOA-TEL Requirements

Req. 1	<p>The WS Addressing specifications, [WS-A 1.0], must include additional fields (in addition to the ones already present) containing remote destinations to which reply messages must be sent.</p> <ul style="list-style-type: none"> <li>• The sender of a message must assign the fields when it wants to specify the destination for the reply message, but the node that has to use such destination information (i.e. the node that has to send the reply message) may not necessarily be the direct receiver of the request message.</li> <li>• The receiver of a message, which needs of information on the endpoint destination to which send a reply message, can obtain the information by these additional fields.</li> <li>• The receiver of a message has to forward to the next receiver all the additional destinations (present in these additional fields) that it does not use.</li> </ul>
Req. 2	<p>The WS-Notification specification must provide a mechanism to describe and regulate a scenario in which one or more intermediaries are present; it must standardize the terminology, concepts, operations, WSDL and XML needed to express the roles of the intermediaries (involved in publish and subscribe Web services for notification message exchange).</p> <p>According to the WS-Notification terminology, the standard must be extended and modified so that:</p> <ul style="list-style-type: none"> <li>• a <i>Subscriber</i> can require a <i>Subscription</i> to a <i>NotificationProducer</i> also in the case they do not communicate directly but do so by means of one or more intermediaries;</li> <li>• likewise a <i>NotificationProducer</i> can send a <i>Notification</i> to a <i>NotificationConsumer</i> also in the case that they do not communicate directly, but by means of one or more intermediaries.</li> </ul>
Req. 3	<p>A new “Message Sender and Receiver concept” must be added in [SOAP 1.2] to model SOAP nodes which must forward the SOAP headers message, but also need to perform changes on the body of the message.</p> <p>A new SOAP protocol must be added to manage the behavior of such nodes.</p>
Req. 4	<p>The WS Security specifications must enable to express a relation between two security tokens, a “main” token (e.g. named “<i>token2</i>”) and a “related” token (e.g. named “<i>token1</i>”).</p> <p>The characteristics of the relation are that, when the token correlation is used,</p> <ul style="list-style-type: none"> <li>• the “main” token can not be built without being in possession of the “related” token,</li> <li>• the WS-Sec header should not be considered valid if the “related” token is not present.</li> </ul> <p>This token correlation requirement defines a new token security model, in which a “main” token is syntactically and semantically meaningful if it is built and presented in relation with another “related” token.</p>
Req. 4.1	<p>It must be possible to express “token correlation” also into the SAML assertion.</p>
Req. 5	<p>In order to make the [SAML 2.0] support name identifier use cases such as that described in section 3.2.1, the Security Services TC must specify a</p> <ul style="list-style-type: none"> <li>• &lt;NameIdentifierRequest&gt; message sent from an Identity Provider to a Service</li> </ul>

	<p>Provider to request a name identifier for a User, and a</p> <ul style="list-style-type: none"> <li>• &lt;NameIdentifierResponse&gt; message sent from the Service Provider to the Identity Provider to return such a name identifier to the Identity Provider.</li> </ul> <p>This requires extensions to the existing [SAML 2.0] core specification (saml-core-2.0-os) including the SAML 2.0 protocol schema. No modification of the existing SAML 2.0 assertion schema is necessary.</p>
Req. 6	<p>In order to make the [SAML 2.0] support attribute management use cases such as that described in 3.3.1, the Security Services TC must specify a</p> <ul style="list-style-type: none"> <li>• &lt;ManageAttributeRequest&gt; message sent from a Service Provider to an Identity Provider to request a modification or the storage of an attribute, and a</li> <li>• &lt;ManageAttributeResponse&gt; message sent from the Identity Provider to the Service Provider to return to the Service Provider the result of processing the received &lt;ManageAttributeRequest&gt; message.</li> </ul> <p>This requires extensions to the existing SAML 2.0 core specification (saml-core-2.0-os) including the SAML 2.0 protocol schema. No modification of the existing SAML 2.0 assertion schema is necessary.</p>
Req. 7	<p>The WS Security specifications must enable to bring two security credentials in the security header: the “main” credential (e.g. named “<i>credential2</i>”) and a “secondary” credential (e.g. named “<i>credential1</i>”).</p> <p>The authentication and authorization process should be performed on the basis of the main credential; the secondary credential should be used to complete the security functionalities.</p>
Req. 7.1	<p>It must be possible to support two credentials also into the SAML assertion.</p>
Req. 8	<p>The SOA Reference Model and Architecture must explain how a service separates and exposes its manageability capabilities to allow other services to manage it.</p> <p>The Service Delivery Framework specified by TM Forum and depicted below sets such requirement at the SDF Service Management Interface.</p>
Req. 9	<p>A standardization body (most probable TM Forum) must normalize the meta-data of Service Management to address the needs of managing any service from a lifecycle perspective. The meta-data should evolve into a meta-model that can be automatically instantiated into current and future management models which are domain (network or IT), technology (enterprise Java, IP network) or lifecycle phase (service creation, deployment, operation, etc).</p>
Req. 10	<p>A common communications profile should be defined such that all multi tier web/mobile applications declaring support for the profile will be able to establish a converged sessions irrespective of the underlying protocols, network domains and access across one or more servers/ services within or across different respective domains.</p> <p>Such a profile will need to define an agreed to approach to:</p> <ol style="list-style-type: none"> <li>1. Establish a session id for the context of converged application.</li> <li>2. Ability to set up event sync supporting a common set of set of bi-directional event classes (i.e. push, broadcast, pub/sub, etc.).</li> <li>3. Universally agreed to means to access the meta-data to discover the interface, binding, events classes, capability of service and device.</li> <li>4. Common and agreed upon means/ nomenclature for an application in real-time to discover, advertise and negotiate device characteristics, codec's and communication modes with a peer or set of peers. <ul style="list-style-type: none"> <li>○ Device attributes, communication protocols and media negotiation achieved through two way services interaction.</li> </ul> </li> </ol>

	This interaction can default to common underlying negotiation means if available/ discoverable at setup time.
--	--

1071