



1

2 **XACML profile for Web-services**

3 **Working draft 02, 23 July 2003**

4 Document identifier: draft-xacml-wspl-02.pdf

5 Location: http://www.oasis-open.org/committees/documents.php?wg_abbrev=xacml

6 Send comments to: xacml-comment@lists.oasis-open.org

7 Editors:

8 Tim Moses, Entrust (tim.moses@entrust.com)

9 Contributors:

10 Anne Anderson, Sun Microsystems

11 Seth Proctor, Sun Microsystems

12 Simon Godik, Overxeer

13 Abstract:

14 This working draft specifies a profile of XACML for expressing policy associated with
15 Web-service end-points.

16 Status:

17 This version of the specification is a working draft of the committee. As such, it is
18 expected to change prior to adoption as an OASIS standard.

19 If you are on the xacml@lists.oasis-open.org list for committee members, send
20 comments there. If you are not on that list, subscribe to the [xacml-comment@lists.oasis-](mailto:xacml-comment@lists.oasis-open.org)
21 [open.org](mailto:xacml-comment@lists.oasis-open.org) list and send comments there. To subscribe, send an email message to [comment-request@lists.oasis-open.org](mailto:xacml-
22 <a href=) with the word "subscribe" as the body of the
23 message.

24

25 Copyright (C) OASIS Open 2003 All Rights Reserved.

26	Table of contents	
27	1. Introduction (non-normative)	4
28	1.1 Glossary	4
29	1.2 Notation	4
30	1.3 Schema organization and namespaces	5
31	1.4 Background	5
32	2. Model (Normative)	5
33	3. Example (Non-normative)	8
34	4. Instructions to standards developers	10
35	4.1 Procedure (Normative)	10
36	4.2 Example (Non-normative)	10
37	5. Definitions (Normative)	11
38	6. End-point policy combination (Normative)	11
39	6.1 Combine top-level <PolicySet> elements	12
40	6.2 Combine second-level <PolicySet> elements	12
41	6.3 Combine <Policy> elements	12
42	6.4 Combine <Rule> elements	12
43	6.5 Combine <Apply> elements	12
44	6.6 Eliminate <Policy> elements	14
45	6.7 Substitute <Apply> elements	15
46	6.8 Result	15
47	7. Security considerations	15
48	8. Bindings (Normative)	15
49	8.1 WSDL 1.1	15
50	8.1.1. Introduction	16
51	8.1.2. Attachment	16
52	8.1.3. Structure	16
53	8.1.4. Integrity/authenticity protection	16
54	8.1.5. Schema	17
55	8.2 WSDL 1.2	19
56	8.3 SOAP 1.1	19
57	8.3.1. Introduction	19
58	8.3.2. Structure	19
59	8.3.3. Integrity/authenticity protection	19
60	8.3.4. Schema	20
61	9. References (Non-normative)	20
62	Appendix A. Worked example (Non-normative)	22
63	Consumer policy	22
64	A.1.1. Plain-language policy	22
65	A.1.2. XACML policy	22
66	Combining process	24
	draft-xacml-wspl-02.pdf	2

67	A.1.3. Combine <PolicySet> elements	24
68	A.1.4. Combine <Policy> elements	26
69	A.1.5. Combine <Rule> elements	28
70	A.1.6. Combine <Apply> elements	31
71	A.1.7. Substitute <Apply> elements	32
72	Appendix B. Revision history	34
73	Appendix C. Notices	35
74		
75		

76 1. Introduction (non-normative)

77 1.1 Glossary

78 **Aspect** – An independent set of technical features and parameters associated with use of a Web-
 79 service. In most cases, an **aspect** is identified with a single member of the suite of Web-service
 80 specifications for which policy provisions must be described, such as WS-Reliable Messaging or
 81 WS-Security. In the former case, policy provisions may include such items as: maximum time to
 82 live, maximum number of retries and minimum interval between retries.

83 **Authorized attribute** – An attribute whose value must be assigned by an authority, not a policy-
 84 user.

85 **Coincidence** – The property of pairs of **predicates**, **strategies**, **objectives** and **end-point**
 86 **policies** that enables them to be combined.

87 **Combiner** – An entity that combines two or more **end-point policies**

88 **Constrained attribute** - An attribute whose value cannot be assigned by the policy-user.

89 **End-point policy** – 1. The set of provisions governing all **aspects** of a Web-service end-point.
 90 2. A conjunctive set of **objectives**. 3. An XACML <PolicySet> element.

91 **Objective** – 1. The set of provisions governing a single **aspect** of a Web-service end-point. 2. A
 92 disjunctive list of **strategies**, in order of preference. 3. An XACML <Policy> element.

93 **Solution** – The set of features and parameter values that satisfy an end-point's requirements for
 94 successful invocation.

95 **Strategy** – 1. One **solution** to a single **aspect** of a Web-service end-point. 2. A conjunctive set
 96 of **predicates**. 3. An XACML <Rule> element.

97 **Unconstrained attribute** - An attribute whose value can be assigned by the policy-user within a
 98 certain range

99 1.2 Notation

100 This specification contains schema conforming to W3C XML Schema and normative text to
 101 describe the syntax and semantics of XML-encoded policy statements.

102 The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD",
 103 "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be
 104 interpreted as described in IETF RFC 2119 [RFC2119]

105 *"they MUST only be used where it is actually required for interoperation or to limit*
 106 *behavior which has potential for causing harm (e.g., limiting retransmissions)"*

107 These keywords are thus capitalized when used to unambiguously specify requirements over
 108 protocol and application features and behavior that affect the interoperability and security of
 109 implementations. When these words are not capitalized, they are meant in their natural-language
 110 sense.

111 `Listings of schemas appear like this.`

112

113 `Example code listings appear like this.`

114 Conventional XML namespace prefixes are used throughout the listings in this specification to
115 stand for their respective namespaces as follows, whether or not a namespace declaration is
116 present in the example:

- 117 • The prefix `xacml`: stands for the XACML policy namespace.
- 118 • The prefix `xs`: stands for the W3C XML Schema namespace [XS].
- 119 • The prefix `xf`: stands for the XQuery 1.0 and XPath 2.0 Function and Operators
120 specification namespace [XF].

121 This specification uses the following typographical conventions in text: `<XACMLElement>`,
122 `<ns:ForeignElement>`, `Attribute`, **Datatype**, `OtherCode`. Terms in *italic bold-face* are
123 intended to have the meaning defined in the Glossary of this document or [XACML v1.0].

124 1.3 Schema organization and namespaces

125 The XACML policy syntax is defined in a schema associated with the following XML namespace:

```
126 urn:oasis:names:tc:xacml:1.0:policy
```

127 1.4 Background

128 Access to a standard-conformant Web-service end-point involves a number of **aspects**, such as:
129 reliable messaging, privacy, authorization, trust, authentication and cryptographic security. Each
130 **aspect** addresses a number of optional features and parameters, which must be coordinated
131 between communicating end-points if the service invocation is to be successful. The provider
132 and consumer of the service likely have different preferences amongst the available choices of
133 features and parameters. Therefore, a mechanism is required by which end-points may describe
134 the mandatory features of service invocation, optional features that they support and the order of
135 their preference amongst such features. Additionally, a procedure is required for combining and
136 reducing these feature descriptions into a service invocation instance that respects both end-
137 points' requirements. These requirements are explained in [WSPL Req].

138 This specification defines a profile of XACML that enables it to be used for describing policy
139 associated with Web-service end-points and using them in a successful invocation.

140 2. Model (Normative)

141 In this profile, an XACML `<PolicySet>` element is associated with a concrete Web-service end-
142 point definition. To that end, its `<Target>` element identifies the WSDL port whose features and
143 parameters it describes. In the case that a policy must be targeted more finely than a port, a
144 second level of `<PolicySet>` whose `<Target>` element identifies the port's operations and
145 messages is inserted. The `<PolicySet>` elements contain `<Policy>` elements that define the
146 **objective** of each **aspect** of policy associated with the port.

147 An XACML `<Policy>` element is associated with a single **aspect** of an **end-point policy**. The
148 `<Target>` element of a `<Policy>` identifies the one **objective** of the **end-point policy** to which
149 it applies. Developers of Web-service specifications that make use of XACML **MUST** define a
150 name and type for its **objective**. In order for an end-point to be successfully invoked, all of its
151 **objectives** **MUST** be achieved by the service invocation. The `<Policy>` element contains
152 `<Rule>` elements that define acceptable alternative **strategies** for achieving the **objective**.

153 An XACML <Rule> element describes one alternative **strategy** for achieving an **objective**. At
154 least one **strategy** MUST be successful if its **objective** is to be achieved. The lexical order of the
155 **strategies** in the **objective** SHOULD reflect the policy-writer's preferences. For example, the
156 policy writer's preferred **strategy** should appear first. The <Rule> element contains a set of
157 <Apply> elements that define **predicates**.

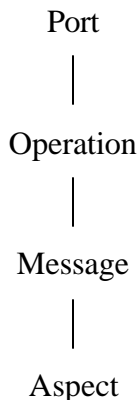
158 An XACML <Apply> element contains one **predicate**. All **predicates** MUST be satisfied by a
159 service invocation if the associated **strategy** is to be successful.

160 An <Apply> element SHALL NOT contain another <Apply> element. It is RECOMMENDED
161 that <Apply> elements be structured as follows:

```
162 <Apply functionId="...">  
163   <AttributeSelector RequestContextPath="..." DataType="..." />  
164   <AttributeValue DataType="..."> ... </AttributeValue>  
165 </Apply>
```

166 In cases where the policy constrains the relationship between attribute values, as opposed to a
167 literal value, it will be necessary to substitute a second <AttributeSelector> element for the
168 <AttributeValue> element in the above fragment. The order of the <AttributeSelector>
169 element and the <AttributeValue> element in the above fragment MAY be reversed to
170 achieve the required constraint if the applied function has no inverse (e.g. subset). Any of the
171 following elements MAY be used in place of the <AttributeSelector> element in either
172 position: <SubjectAttributeDesignator>, <ResourceAttributeDesignator>, <ActionAttributeDesignator> or <EnvironmentAttributeDesignator>.

174 The relevant portion of the WSDL data model is hierarchical, as shown in Figure 1.
175



176
177

Figure 1 - WSDL hierarchical data model

178 This structure is reflected in the **end-point policy** model, as shown in Figure 2.
179 Names assigned to objects in the WSDL model are used in <Target> elements of the **end-point**
180 **policy** to associate policy statements with those objects. The names are considered
181 structureless. That is, the name of an object does not reflect its location in the WSDL hierarchy.
182 Nevertheless, a <Target> element used to associate a policy statement with a non-root object in
183 the WSDL model is intended to identify the object within the context established by the
184 <Target> elements of its enclosing <PolicySet> elements. So, target matching SHALL be
185 performed on the set of objects that has been successively refined by outer layers of the **end-**
186 **point policy**.

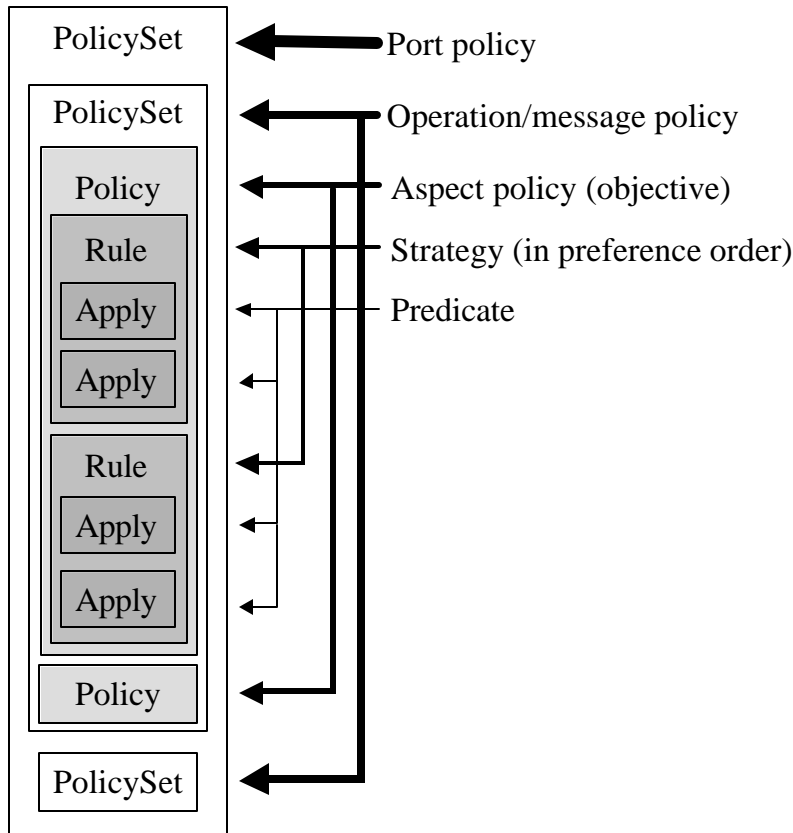


Figure 2 – End-point policy model

187

188

189 This model has been chosen to facilitate combining of *end-point policies*.

190 The following consequences flow from the model:

- 191 1. The policy-combining algorithm for <PolicySet> elements SHALL be
192 "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides".
- 193 2. The contents of all <PolicySet/Target/Subjects> elements SHALL be
194 <AnySubject/>.
- 195 3. The contents of the top-level <PolicySet/Target/Resources> element SHALL be
196 the name attribute of the end-point's port definition.
- 197 4. The contents of the top-level <PolicySet/Target/Actions> element SHALL be
198 <AnyAction/>.
- 199 5. If present, the contents of the second-level <PolicySet/Target/Resources>
200 element SHALL either be the name attribute of the end-point's message definition or the
201 element <AnyResource/>.
- 202 6. If present, the contents of the second-level <PolicySet/Target/Actions> element
203 SHALL be the name attribute of the end-point's operation definition or the element
204 <AnyAction/>.
- 205 7. If the contents of the second-level <PolicySet/Target/Resources> element is the
206 element <AnyResource/>, then the contents of the <PolicySet/Target/Actions>
207 element SHALL NOT be the element <AnyAction/>, and vice-versa. Otherwise, its

208 <Policy> elements should be placed immediately subordinate to the top-level
209 <PolicySet> element.

210 8. The rule-combining algorithm for a <Policy> element SHALL be
211 "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-overrides".

212 9. The MatchId for the <Policy/Target/Resources> element SHALL be
213 "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal".

214 10. The Effect attribute of all <Rule> elements SHALL be "Permit".

215 11. The contents of the <Policy/Target/Subjects> element SHALL be
216 <AnySubject/>.

217 12. The contents of the <Policy/Target/Resources> element SHALL be
218 <AnyResource/>.

219 13. The contents of the <Policy/Target/Actions> element SHALL identify the
220 **objective** (see Section 4).

221 14. The <Rule/Target> element SHALL be omitted.

222 15. The FunctionId attribute of a <Condition> element SHALL be
223 "urn:oasis:names:tc:xacml:1.0:function:and".

224 16. The FunctionId attribute of an <Apply> element SHALL identify one of the matching
225 functions specified in XACML.

226 In order to be considered conformant with this profile, a <PolicySet> element MUST satisfy all
227 of these conditions.

228 3. Example (Non-normative)

229 This section contains an example of a service-provider policy on the **aspect** of data-rate
230 allocation.

231 Here is a plain-language description of the policy.

232 Clients paying €150/minute are allocated a guaranteed minimum data-rate of 64kb/s.

233 Clients paying €45/minute are allocated a guaranteed minimum data-rate between 6pm
234 and midnight of 40kb/s.

235 In order to make the example somewhat easier to read, several abbreviations have been
236 introduced. For instance:

237 The <Subjects> element has been omitted from all the <Target> elements.

238 Only <*Match> elements have been retained in <Target> elements.

239 URIs have been abbreviated.

240 "*one-and-only" bag functions have been omitted around <AttributeDesignator>
241 elements in <Condition> elements.

242 Data Type and FunctionId prefixes have been omitted. A reader familiar with XACML
243 should be able to reconstruct a syntactically correct policy from the information provided.

```
244 <?xml version="1.0" encoding="UTF-8"?>  
245 <PolicySet PolicySetId="Provider Policy"  
246 PolicyCombiningAlgId="deny-overrides">
```



```

247 <Target>
248   <Resources>
249     <ResourceMatch MatchId="equal"
250       <AttributeValue DataType="anyURI">
251         serviceX:portX
252       </AttributeValue>
253       <ResourceAttributeDesignator AttributeId="portID"
254   DataType="anyURI" />
255     </ResourceMatch>
256   </Resources>
257   <Actions>
258     <AnyAction />
259   </Actions>
260 </Target>
261 <Policy PolicyId="Provider Data-Rate Allocation Objective"
262   RuleCombiningAlgId="permit-overrides">
263   <Target>
264     <Actions>
265       <ActionMatch MatchId="equal">
266         <AttributeValue DataType="anyURI">
267           data-rate-allocation
268         </AttributeValue>
269         <ActionAttributeDesignator AttributeId="objectiveId"
270   DataType="anyURI" />
271       </ActionMatch>
272     </Actions>
273   </Target>
274   <Rule RuleId="Provider Data-Rate Allocation Objective Strategy
275   1" Effect="Permit">
276     <Condition FunctionId="and">
277       <Apply FunctionId="equal">
278         <SubjectAttributeDesignator DataType="integer"
279   AttributeId="fee" />
280         <AttributeValue DataType="integer">
281           150
282         </AttributeValue>
283       </Apply>
284       <Apply FunctionId="greater-than-or-equal">
285         <ResourceAttributeDesignator DataType="integer"
286   AttributeId="data-rate" />
287         <AttributeValue DataType="integer">
288           64000
289         </AttributeValue>
290       </Apply>
291     </Condition>
292   </Rule>
293   <Rule RuleId="Provider Data-Rate Allocation Objective Strategy
294   2" Effect="Permit">
295     <Condition FunctionId="and">
296       <Apply FunctionId="equal">
297         <SubjectAttributeDesignator DataType="integer"
298   AttributeId="fee" />
299         <AttributeValue DataType="integer">
300           45
301         </AttributeValue>
302       </Apply>
303       <Apply FunctionId="equal">
304         <ResourceAttributeDesignator DataType="integer"
305   AttributeId="data-rate" />

```

```

306         <AttributeValue DataType="integer">
307             40000
308         </AttributeValue>
309     </Apply>
310     <Apply FunctionId="greater-than-or-equal">
311         <EnvironmentAttributeDesignator DataType="time"
312 AttributeId="timeOfDay"/>
313         <AttributeValue DataType="time">
314             18:00
315         </AttributeValue>
316     </Apply>
317 </Condition>
318 </Rule>
319 </Policy>
320 </PolicySet>

```

321 4. Instructions to standards developers

322 Developers of Web-services standards that are intended to conform with this profile MUST define
323 standard-specific policy parameters.

324 4.1 Procedure (Normative)

325 Developers of Web-services standards MUST complete the following steps.

- 326 1. Assign a URI for at least one `objectiveId` attribute. In the event that the specification
327 document-identifier is a URI, it MAY be used as the `objectiveId` URI.
- 328 2. Define a set of attribute names, types and semantics.
- 329 3. Select matching functions on the attributes from the matching functions defined in
330 **[XACML]**. The functions MUST be type-consistent with the attributes. For every
331 individual attribute, its associated matching functions MUST be combinable, as defined in
332 Table 1. It is RECOMMENDED to use *type-greater-than-or-equal* or *type-less-than-or-*
333 *equal* matching functions in preference to *type-greater-than* or *type-less-than* matching
334 functions, respectively.

335 These attributes and functions MAY be used in *predicates*.

336 4.2 Example (Non-normative)

337 A committee defining the reliable messaging *aspect* of Web-service invocation might assign the
338 URI:

```

339
340     urn:oasis:names:tc:wsm:1.0:objectiveId

```

341
342 as the `objectiveId`.

343 It might identify the *maximum-time-to-live* **attribute** as a parameter of policy. It might assign the
344 identifier:

```

345
346     urn:oasis:names:tc:wsm:1.0:maximum-time-to-live

```

347
348 to this attribute. Then it might identify the attribute type to be
349
350 <http://www.w3.org/TR/2002/WD-xquery-operators-20020816#DayTimeDuration>.
351
352 It might define its meaning to be the maximum value permitted to be assigned by the requestor to
353 the “time-to-live” parameter associated with a service request. Then it might identify
354
355 <urn:oasis:names:tc:xacml:1.0:function:dateTime-less-than-or-equal>
356
357 as the matching function associated with the *attribute*.
358 The committee MUST specify all relevant parameters in a similar way.

359 5. Definitions (Normative)

360 This profile defines one attribute.
361 Name: <urn:oasis:names:tc:xacml:1.0:attribute:objectiveId>.
362 Type: <xs:anyURI>.
363 Meaning: the value of this attribute indicates the *aspect* of policy addressed by a `<Policy>`
364 element. The
365 `Policy/Target/Actions/ActionMatch/ActionAttributeDesignator@AttributeId`
366 attribute MUST be assigned this value.

367 6. End-point policy combination (Normative)

368 The need to combine two or more policies is described in [WSPL Req].
369 The procedure for combining two top-level `<PolicySet>` elements is described here. More than
370 two `<PolicySet>` elements MAY be combined by repeating this procedure. Alternative
371 procedures that achieve the same result under all circumstances SHALL be considered
372 conformant.
373 The combining procedure involves combining *coincident* top-level `<PolicySet>` elements, then
374 combining *coincident* second-level `<PolicySet>` elements within the combined top-level
375 `<PolicySet>` elements, then combining *coincident* `<Policy>` elements within the combined
376 `<PolicySet>` elements, then combining *coincident* `<Rule>` elements within the combined
377 `<Policy>` elements and finally combining *coincident* `<Apply>` elements within the combined
378 `<Rule>` elements. Finally, elimination and substitution steps are applied.
379 The detailed steps are described below.
380 The effect of this procedure is to identify a single `<Rule>` element for each *objective* that
381 represents the contract between the parties. The contract is compatible with both of the original
382 *end-point policies*, while reflecting the preferences of the *combiner*.

383

6.1 Combine top-level <PolicySet> elements

384 Combine **coincident** top-level <PolicySet> elements. <PolicySet> elements are
385 **coincident** if and only if their <Target> elements are identical.

386 In order to combine two top-level <PolicySet> elements, append the foreign <Policy> and
387 second-level <PolicySet> elements to the **combiner's**<Policy> and second-level
388 <PolicySet> elements and assign a new unique PolicySetId attribute.

389

6.2 Combine second-level <PolicySet> elements

390 If second-level <PolicySet> elements are present, then all **coincident** pairs of these MUST be
391 combined in the same way. If a second-level <PolicySet/Target/Resources> element
392 contains the <AnyResource/> element, then it is **coincident** with another second-level
393 <PolicySet> element if and only if their <Target/Actions> elements are identical. The
394 converse is the case if the <AnyAction> element is present.

395

6.3 Combine <Policy> elements

396 Within the resulting <PolicySet> elements, combine all **coincident** <Policy> elements.
397 <Policy> elements are **coincident** if and only if their <Target> elements are identical.

398 In order to combine two <Policy> elements, append the foreign <Rule> elements to the
399 **combiner's**<Rule> elements and assign a new unique PolicyId attribute.

400

6.4 Combine <Rule> elements

401 Within each resulting <Policy> element, combine <Rule> elements in all possible pairings,
402 taking one from the **combiner's**set and one from the foreign set. The **combiner's**first
403 <Policy> element SHOULD be paired with each of the foreign <Policy> elements, starting
404 with the first, then the **combiner's**second <Policy> element SHOULD be paired with each of
405 the foreign <Policy> elements, etc.. This procedure respects the preferences of each policy
406 writer, while giving priority to those of the **combiner**.

407 In order to combine two <Rule> elements, append the <Apply> elements from the foreign
408 <Rule> element to the **combiner's**<Apply> elements and assign a new unique RuleId
409 attribute.

410

6.5 Combine <Apply> elements

411 Within each resulting <Rule> element, combine all **coincident** <Apply> elements. <Apply>
412 elements are **coincident** if they constrain the same attribute. If there exists no attribute value for
413 which both <Apply> elements evaluate to "True", then their **strategies** are incompatible and the
414 <Rule> element MUST be discarded. The test for compatible strategies is shown in the third
415 column of Table 1. If no <Rule> elements remain, then the procedure SHALL terminate in
416 failure. Note that in the case where the same attribute is constrained by different **aspects**, this
417 procedure will not detect incompatible constraints.

418 **Coincident** <Apply> elements SHALL be combined as shown in the fourth column of Table 1.

419 Table 1 is to be interpreted according to the following key.

- 420 1. Columns one, two and four contain shorthand versions of an XACML <Apply> element.
421 The portion before the open parenthesis (e.g. "type-equal" in the first row) represents the

- 422 <Apply> element's FunctionId attribute value. The "type-" portion represents any of
 423 the type-specific parts of the standard XACML function identifiers.
- 424 2. Alphabetic symbols (e.g. "a" in the first row) represent XACML
 425 <AttributeDesignator>, <AttributeSelector> or <AttributeValue>
 426 elements.
- 427 3. Where N/A appears in the fourth column there is no single replacement <Apply>
 428 element.
- 429 4. \lceil means the smallest value greater than.
- 430 5. \lfloor means the largest value less than.
- 431 6. \cap means set intersection.
- 432 7. \subset means "is a proper subset of".

First <Apply> element	Second <Apply> element	Compatible strategies	Replacement <Apply> element
<i>type-equal</i> (a,b)	<i>type-equal</i> (a,c)	$b == c$	<i>type-equal</i> (a,b)
<i>type-equal</i> (a,b)	<i>type-greater-than</i> (a,c)	$b > c$	<i>type-equal</i> (a,b)
<i>type-equal</i> (a,b)	<i>type-greater-than-or-equal</i> (a,c)	$b = c$	<i>type-equal</i> (a,b)
<i>type-equal</i> (a,b)	<i>type-less-than</i> (a,c)	$b < c$	<i>type-equal</i> (a,b)
<i>type-equal</i> (a,b)	<i>type-less-than-or-equal</i> (a,c)	$b = c$	<i>type-equal</i> (a,b)
<i>type-greater-than</i> (a,b)	<i>type-greater-than</i> (a,c)		<i>type-greater-than</i> (a,max(b,c))
<i>type-greater-than</i> (a,b)	<i>type-greater-than-or-equal</i> (a,c)		<i>type-greater-than-or-equal</i> (a,max(\lceil b,c))
<i>type-greater-than-or-equal</i> (a,b)	<i>type-greater-than-or-equal</i> (a,c)		<i>type-greater-than-or-equal</i> (a,max(b,c))
<i>type-less-than</i> (a,b)	<i>type-less-than</i> (a,c)		<i>type-less-than</i> (a,min(b,c))
<i>type-less-than</i> (a,b)	<i>type-less-than-or-equal</i> (a,c)		<i>type-less-than-or-equal</i> (a,min(\lfloor b,c))
<i>type-less-than-or-equal</i> (a,b)	<i>type-less-than-or-equal</i> (a,c)		<i>type-less-than-or-equal</i> (a,min(b,c))
<i>type-greater-than</i> (a,b)	<i>type-less-than</i> (a,c)	$b < c$	N/A
<i>type-greater-than</i> (a,b)	<i>type-less-than-or-equal</i> (a,c)	$b < c$	N/A
<i>type-greater-than-or-equal</i> (a,b)	<i>type-less-than</i> (a,c)	$b < c$	N/A
<i>type-greater-than-or-</i>	<i>type-less-than-or-</i>	$b < c$	N/A

equal(a,b)	equal(a,c)		
set-equals(a,b)	set-equals(a,c)	b == c	set-equals(a,b)
set-equals(a,b)	subset(a,c)	b ? c	set-equals(a,b)
subset(a,b)	subset(a,c)	n (b,c) ? 0	subset (a, n (b,c))

433 **Table 1 - Predicate combination**

434 **6.6 Eliminate <Policy> elements**

435 Following combination, an elimination step MUST be applied. The <Rule> elements represent
 436 the available **strategies** in order of preference for each **aspect**. Ideally, the policy-user would
 437 adopt the first <Rule> element as its **strategy** for invoking the service. However, some
 438 **strategies** may place constraints on attributes that are not within the control of the policy-user.
 439 Such strategies MUST be eliminated.

440 The policy-user MUST categorize attributes according to the degree of control it has over their
 441 assigned values. **Constrained attributes** are ones over which the policy-user has no control.
 442 **Unconstrained attributes** are ones whose values it can assign within a certain range.

443 **Authorized attributes** are ones that must be assigned by an authority, not the policy-user.

444 Elimination proceeds by examining each <Apply> element, as described below.

- 445 1. If the <Apply> element places a literal constraint on a **constrained attribute**, then the
 446 policy-user SHALL test whether the constraint is satisfied by the attribute. If it is, then it
 447 SHALL proceed. If it is not, then the enclosing <Rule> element SHALL be eliminated. Some
 448 constrained attributes vary with time. The policy-user MAY wait until the attribute adopts the
 449 required value. In the case of the environmental attribute: "time", it will never again adopt
 450 values in the past. Values in the future will arise in a predictable manner.
- 451 2. If the <Apply> element places a literal constraint on an **unconstrained attribute**, then the
 452 policy-user SHALL assign a value to the attribute that satisfies the constraint. If the required
 453 value is not in the available range, then the enclosing <Rule> element SHALL be eliminated.
- 454 3. If the <Apply> element constrains the relationship between two **constrained attributes**,
 455 then the policy-user SHALL test whether the constraint is satisfied by the attributes. If it is,
 456 then it SHALL proceed. If it is not, then the enclosing <Rule> element SHALL be eliminated.
- 457 4. If the <Apply> element constrains the relationship between two **unconstrained attributes**,
 458 then the policy-user SHALL assign a value to one or both of the attributes that satisfies the
 459 constraint. If the required value is not in the available range, then the enclosing <Rule>
 460 element SHALL be eliminated.
- 461 5. If the <Apply> element constrains the relationship between a **constrained attribute** and an
 462 **unconstrained attribute**, then the policy-user SHALL assign a value to the **unconstrained**
 463 **attribute** that satisfies the constraint. If the required value is not in the available range, then
 464 the enclosing <Rule> element SHALL be eliminated.
- 465 6. If the <Apply> element constrains **authorized attributes**, then the policy-user SHALL obtain
 466 the required attribute from an acceptable authority. The **strategy** containing the attribute
 467 constraint should also indicate what constitutes an acceptable authority. If the required
 468 attribute cannot be obtained, then the enclosing <RULE> element SHALL be eliminated.

469 <Rule> elements MUST be examined in order until one survives the elimination procedure. This
 470 represents the highest preference **strategy** with which the policy-user is able to comply.
 471 Therefore, this (and only this) one SHALL be retained.
 472 If, after completing the elimination step, no <Rule> elements remain, then the procedure SHALL
 473 terminate in failure.

474 6.7 Substitute <Apply> elements

475 Following elimination, a substitution step MAY be applied to the <Apply> element of the
 476 remaining <Rule> element. Substitution proceeds by the following steps. The substitutions
 477 shown in Table 2 SHALL be applied.

<Apply> element	Replacement <Apply> element
<i>type-greater-than(a,b)</i>	<i>type-equal(a, ⊔ b)</i>
<i>type-greater-than-or-equal(a,b)</i>	<i>type-equal(a,b)</i>
<i>type-less-than(a,b)</i>	<i>type-equal(a, ⊓ b)</i>
<i>type-less-than-or-equal(a,b)</i>	<i>type-equal(a,b)</i>
<i>type-subset(a,b)</i>	<i>set-equals(a,b)</i>

478 **Table 2 – Substitution procedure**

479 6.8 Result

480 The result of this procedure is a set of **strategies**, one for each **aspect** of service policy, and
 481 each containing value assignments for attributes that are under the control of the policy-user. A
 482 service invocation using these attribute assignments conforms with the applicable policy of both
 483 the consumer and the provider.

484 7. Security considerations

485 Policies SHALL be integrity protected. The policy-user MUST confirm that the author of the policy
 486 is an entity that is authoritative for the target end-point. How this is achieved is outside the scope
 487 of this specification.

488 8. Bindings (Normative)

489 <PolicySet> elements MAY be distributed in a [WSDL 1.1] or WSDL 1.2 service description or
 490 in a [SOAP 1.1] message. When they are distributed by one of these means, they MUST be
 491 distributed as defined in this section.

492 8.1 WSDL 1.1

493 This section defines how <PolicySet> elements SHALL be included in a WSDL 1.1 service
 494 description for a Web-service end-point.

495

8.1.1. Introduction

496 As a precursor to invoking a WSDL operation of a WSDL port, certain consumer configuration
497 steps are likely to be required, and these configuration steps are likely to be associated with the
498 port, rather than with an individual operation. Locating, retrieving, validating and combining policy
499 are appropriate functions to perform as one of these configuration steps.

500 Different **aspects** of policy may be most applicable to different objects within the WSDL data
501 model, see Figure 1. For instance, privacy policy may apply to a WSDL message definition,
502 regardless of which WSDL operation uses the message. Crypto-security policy, on the other
503 hand, may apply to a message definition, differently, according to which operation uses the
504 message. And, trust policy may apply to the port, independent of which operation or message is
505 used.

506

8.1.2. Attachment

507 For the reasons stated in Section 8.1.1, a top-level `<PolicySet>` element SHALL be targeted
508 only at a WSDL port. However, it MUST be possible to associate a policy statement with any
509 object (port, operation or message) either alone or in combination, see Figure 2. For this reason,
510 policy statements MUST be capable of differentiating between the various WSDL operation and
511 message definitions of the WSDL port at which they are targeted.

512 The WSDL schema requires that `<wsdl/port>`, `<wsdl/operation>` and `<wsdl/message>`
513 elements have a `name` attribute of type `NCName`. This attribute is used to associate policies with
514 a particular port, operation or message or combinations thereof. URLs are a form of `NCName`.

515

8.1.3. Structure

516 Conformant `<PolicySet>` elements SHALL be structured as follows:

517 The top-level element SHALL be a `<PolicySet>` element whose
518 `<PolicySet/Target/Resources>` element identifies the WSDL port to which it is applicable,
519 by means of the `wsdl/port@name` attribute.

520 Policies that apply to the WSDL port, regardless of the particular operation or message SHALL be
521 contained in `<Policy>` elements immediately subordinate to the top-level `<PolicySet>`
522 element.

523 Policies that apply to some combination of WSDL port, operation and message SHALL be
524 contained in `<PolicySet>` elements subordinate to the top-level `<PolicySet>` element.

525 These second-level `<PolicySet>` elements SHALL have `<PolicySet/Target/Actions>`
526 elements that identify the WSDL operation, and `<PolicySet/Target/Resources>` elements
527 that identify the WSDL message to which they are applicable, by means of the
528 `wsdl/operation@name` and `wsdl/message@name` attributes, respectively. Only WSDL
529 message definitions of the "input" type SHALL be identified.

530 The `<Policy/Target/Resources>` element SHALL identify the **aspect** of policy to which it
531 applies.

532

8.1.4. Integrity/authenticity protection

533 If the `<wsdl/definitions>` element is integrity-protected, then the `<PolicySet>` elements
534 SHOULD be included within the integrity-protection of that element.

535 Where it is not possible to do this, either because the `<wsdl/definitions>` element is not
536 integrity-protected, or for other reasons, `<PolicySet>` elements SHALL be enclosed in a

537 <saml/Assertion> element wrapper **[SAML]**. This allows supporting information, such as the
538 saml/Assertion@Issuer attribute to be attached. The <saml/Assertion> element SHALL
539 be integrity-protected.

540 The policy-user SHALL ignore the PolicySet@PolicySetId attribute.

541 The WSDL port to which a policy applies SHALL be identified in the top-level
542 <PolicySet/Target/Resources> element, by means of the wsdl/port@name attribute.
543 The policy-user SHALL confirm that it has located the correct policy by examining the policy's top-
544 level <PolicySet/Target/Resources> element Furthermore, if they are present, the policy-
545 user SHALL confirm that the policy is current, by examining the
546 saml/Assertion/Conditions@NotBefore and
547 saml/Assertion/Conditions@NotOnOrAfter attributes.

548 The wsdl/port@name attribute SHALL contain a URL. In the case where a policy is wrapped in
549 a <saml/Assertion>, the host and domain parts of the wsdl/port@name URL SHALL be
550 identical to the saml/Assertion@Issuer attribute value. The saml/Assertion@Issuer
551 attribute value SHALL be identical to the CN attribute value in the subject field of the certificate
552 **[X509]** that validates the <saml/Assertion> element, whether integrity protection is provided
553 by SSL or XML Digital Signature.

554 8.1.5. Schema

555 A <PolicySet> element SHALL be included in a <wsdl/definitions> element in
556 accordance with the following schema. Additions to the WSDL 1.1 SOAP binding are highlighted.

```

557 <?xml version="1.0" encoding="UTF-8"?>
558 <schema targetNamespace="http://schemas.xmlsoap.org/wsdl/policy-
559 conformant-soap/" xmlns="http://www.w3.org/2001/XMLSchema"
560 xmlns:policy-conformant-
561 soap="http://schemas.xmlsoap.org/wsdl/policy-conformant-soap/"
562 xmlns:xacml="urn:oasis:names:tc:xacml:1.0:policy">
563   <import namespace="urn:oasis:names:tc:xacml:1.0:policy"
564   schemaLocation="http://www.oasis-
565 open.org/committees/download.php/915/cs-xacml-schema-policy-
566 01.xsd"/>
567   <element name="EndPointPolicy" type="xacml:PolicySetType"/>
568   <element name="binding" type="policy-conformant-
569 soap:bindingType"/>
570   <complexType name="bindingType">
571     <attribute name="transport" type="anyURI" use="optional"/>
572     <attribute name="style" type="policy-conformant-
573 soap:styleChoice" use="optional"/>
574   </complexType>
575   <simpleType name="styleChoice">
576     <restriction base="string">
577       <enumeration value="rpc"/>
578       <enumeration value="document"/>
579     </restriction>
580   </simpleType>
581   <element name="operation" type="policy-conformant-
582 soap:operationType"/>
583   <complexType name="operationType">
584     <attribute name="soapAction" type="anyURI" use="optional"/>
585     <attribute name="style" type="policy-conformant-
586 soap:styleChoice" use="optional"/>
587

```

```

588 </complexType>
589 <element name="body" type="policy-conformant-soap:bodyType"/>
590 <complexType name="bodyType">
591   <attribute name="encodingStyle" type="anyURI" use="optional"/>
592   <attribute name="parts" type="NMTOKENS" use="optional"/>
593   <attribute name="use" type="policy-conformant-soap:useChoice"
594 use="optional"/>
595   <attribute name="namespace" type="anyURI" use="optional"/>
596 </complexType>
597 <simpleType name="useChoice">
598   <restriction base="string">
599     <enumeration value="literal"/>
600     <enumeration value="encoded"/>
601   </restriction>
602 </simpleType>
603 <element name="fault" type="policy-conformant-soap:faultType"/>
604 <complexType name="faultType">
605   <complexContent>
606     <restriction base="policy-conformant-soap:bodyType">
607       <attribute name="parts" type="NMTOKENS" use="prohibited"/>
608     </restriction>
609   </complexContent>
610 </complexType>
611 <element name="header" type="policy-conformant-
612 soap:headerType"/>
613 <complexType name="headerType">
614   <all>
615     <element ref="policy-conformant-soap:headerfault"/>
616   </all>
617   <attribute name="message" type="QName" use="required"/>
618   <attribute name="parts" type="NMTOKENS" use="required"/>
619   <attribute name="use" type="policy-conformant-soap:useChoice"
620 use="required"/>
621   <attribute name="encodingStyle" type="anyURI" use="optional"/>
622   <attribute name="namespace" type="anyURI" use="optional"/>
623 </complexType>
624 <element name="headerfault" type="policy-conformant-
625 soap:headerfaultType"/>
626 <complexType name="headerfaultType">
627   <attribute name="message" type="QName" use="required"/>
628   <attribute name="parts" type="NMTOKENS" use="required"/>
629   <attribute name="use" type="policy-conformant-soap:useChoice"
630 use="required"/>
631   <attribute name="encodingStyle" type="anyURI" use="optional"/>
632   <attribute name="namespace" type="anyURI" use="optional"/>
633 </complexType>
634 <element name="address" type="policy-conformant-
635 soap:addressType"/>
636 <complexType name="addressType">
637   <attribute name="location" type="anyURI" use="required"/>
638 </complexType>
639 <element name="port" type="wsdl:portType"/>
640 <complexType name="portType">
641   <complexContent>
642     <extension base="wsdl:documented">
643       <sequence>
644         <any namespace="##other" minOccurs="0"/>
645         <element ref="xacml:PolicySetIdReference"/>
646       </sequence>

```

647
648
649
650
651
652

```
<attribute name="name" type="NCName" use="required"/>  
<attribute name="binding" type="QName" use="required"/>  
</extension>  
</complexContent>  
</complexType>  
</schema>
```

653

8.2 WSDL 1.2

654 This section defines how `<PolicySet>` elements are included in a WSDL 1.2 service description
655 for a Web-service end-point. TBD

656

8.3 SOAP 1.1

657

8.3.1. Introduction

658 In the case of a WSDL request-response-operation, consumer policies for the response message
659 MAY be conveyed in a SOAP header of the corresponding request message. The names
660 assigned to objects by the consumer are not guaranteed to match those assigned by the provider
661 to the equivalent objects. Therefore, the consumer MUST use the names assigned by the
662 provider to associate consumer policy with WSDL objects. This means that response policies
663 MUST be tailored to the particular provider, and the consumer may require a different policy for
664 each provider of the same service.

665 In the case of the WSDL solicit-response-operation and the notification-operation, the WSDL
666 technique, described above, SHALL be used to disseminate consumer policy.

667

8.3.2. Structure

668 Conformant `<PolicySet>` elements SHALL be structured as described in Section 8.1.3, above.
669 Only WSDL message definitions of the "output" or "fault" types SHALL be targeted by policies.

670

8.3.3. Integrity/authenticity protection

671 If the `<soap/header>` element is integrity-protected, then the `<PolicySet>` elements
672 SHOULD be included within the integrity-protection of that element.

673 Where it is not possible to do this, either because the `<soap/header>` element is not integrity-
674 protected, or for other reasons, `<PolicySet>` elements SHALL be enclosed in a
675 `<saml/Assertion>` element wrapper [SAML]. The `<saml/Assertion>` element SHALL be
676 integrity protected.

677 The policy-user SHALL ignore the `PolicySet@PolicySetId` attribute.

678 The policy-user SHALL verify that the `<PolicySet/Target>` element identifies the
679 `wsdl/port@name` attribute of the WSDL port that originated the request.

680 In the case where a policy is wrapped in a `<saml/Assertion>`, the host and domain parts of
681 the authenticated name of the originating end-point SHALL be identical to the
682 `saml/Assertion@Issuer` attribute value. The `saml/Assertion@Issuer` attribute value
683 SHALL be identical to the CN attribute value in the subject field of the certificate [X509] that
684 validates the `<saml/Assertion>` element, whether integrity protection is provided by SSL or
685 XML Digital Signature.

686 If they are present, the policy-user SHALL confirm that the policy is current, by examining the
687 saml/Assertion/Conditions@NotBefore and
688 saml/Assertion/Conditions@NotOnOrAfter attributes.

8.3.4. Schema

690 An XACML <PolicySet> element SHALL be included in a SOAP header in accordance with the
691 following schema.

```
692 <?xml version="1.0" encoding="UTF-8"?>
693 <xs:schema
694   targetNamespace="urn:oasis:names:tc:xacml:wspl:draft:02"
695   xmlns:EndPointPolicy="urn:oasis:names:tc:xacml:wspl:draft:02"
696   xmlns:xs=http://www.w3.org/2001/XMLSchema
697   xmlns:xacml="urn:oasis:names:tc:xacml:1.0:policy"
698   xmlns:SOAP-ENV=http://schemas.xmlsoap.org/soap/envelope/
699   elementFormDefault="qualified" attributeFormDefault="unqualified">
700   <xs:import namespace=http://schemas.xmlsoap.org/soap/envelope/
701     schemaLocation="http://schemas.xmlsoap.org/soap/envelope/" />
702   <xs:import namespace="urn:oasis:names:tc:xacml:1.0:policy"
703     schemaLocation="http://www.oasis-
704     open.org/committees/download.php/915/cs-xacml-schema-policy-
705     01.xsd" />
706   <xs:element name="Policy" type="EndPointPolicy:PolicyType" />
707   <xs:complexType name="PolicyType">
708     <xs:complexContent>
709       <xs:extension base="SOAP-ENV:Header">
710         <xs:sequence>
711           <xs:element ref="xacml:PolicySet" />
712         </xs:sequence>
713       </xs:extension>
714     </xs:complexContent>
715   </xs:complexType>
716 </xs:schema>
```

9. References (Non-normative)

- 717
- 718 **[RFC2119]** S. Bradner, Key words for use in RFCs to Indicate Requirement Levels, IETF
719 RFC 2119, March 1997. Located at: <http://www.ietf.org/rfc/rfc2119.txt>
- 720 **[SAML]** Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML)
721 OASIS Standard, 5 November 2002. Located at: [http://www.oasis-
open.org/committees/download.php/1371/oasis-sstc-saml-core-1.0.pdf](http://www.oasis-
722 open.org/committees/download.php/1371/oasis-sstc-saml-core-1.0.pdf)
- 723 **[SOAP 1.1]** Simple Object Access Protocol (SOAP) 1.1, W3C Note 08 May 2000. Located
724 at: http://www.w3.org/TR/SOAP/#_Toc478383497
- 725 **[WSDL 1.1]** Web Services Description Language (WSDL) 1.1, W3C Note 15 March 2001.
726 Located at: <http://www.w3.org/TR/wsdl#A4.2>
- 727 **[WSPL Req]** Web-services policy language use-cases and requirements, working draft 01, 7
728 March 2003. Located at: <http://lists.oasis-open.org/archives/xacml/200303/msg00014.html>
- 729 **[X509]** ITU-T Recommendation X.509 version 3 (1997). "Information Technology – Open
730 System Interconnection – The Directory Authentication Framework" ISO/IEC 9594-1:1997
- 731 **[XACML v1.0]** eXtensible Access Control Markup Language (XACML) Version 1.0
draft-xacml-wspl-02.pdf

732 OASIS Standard, 18 February 2003. Located at: <http://www.oasis->
733 [open.org/committees/xacml/repository/](http://www.oasis-open.org/committees/xacml/repository/)

734 **[XF]** XQuery 1.0 and XPath 2.0 Functions and Operators, W3C Working Draft 16 August
735 2002. Available at: <http://www.w3.org/TR/2002/WD-xquery-operators-20020816>

736 **[XS]** XML Schema, parts 1 and 2. Available at: <http://www.w3.org/TR/xmlschema-1/> and
737 <http://www.w3.org/TR/xmlschema-2/>

Appendix A. Worked example (Non-normative)

738

739

740 This appendix contains a worked example to illustrate the process of combining and reducing
741 XACML policies that conform with this profile, using two simple policy instances. The example is
742 drawn from the realm of data-rate allocation, and builds on the example given in Section 3.

743 Consumer policy

744 This section describes the service consumer's requirements for the data-rate allocation *aspect* of
745 service invocation.

746 A.1.1. Plain-language policy

747 The plain language description of the policy is as follows.

748 The service-consumer's first choice is to pay a maximum of €100/minute for a minimum
749 guaranteed data-rate of 64kb/s.

750 The second choice is to pay a maximum of €50/minute for a minimum guaranteed data-
751 rate between 9pm and midnight of 32kb/s.

752 A.1.2. XACML policy

```
753 <PolicySet PolicySetId="Consumer Policy"  
754 PolicyCombiningAlgId="deny-overrides">  
755   <Target>  
756     <Resources>  
757       <ResourceMatch MatchId="equal"  
758         <AttributeValue DataType="anyURI">  
759           serviceX:portX  
760         </AttributeValue>  
761         <ResourceAttributeDesignator AttributeId="portID"  
762         DataType="anyURI" />  
763       </ResourceMatch>  
764     </Resources>  
765     <Actions>  
766       <AnyAction/>  
767     </Actions>  
768   </Target>  
769   <Policy PolicyId="Consumer Data-Rate Allocation Objective"  
770     RuleCombiningAlgId="permit-overrides">  
771     <Target>  
772       <Actions>  
773         <ActionMatch MatchId="equal">  
774           <AttributeValue DataType="anyURI">  
775             data-rate-allocation  
776           </AttributeValue>
```

```

777         <ActionAttributeDesignator AttributeId="objectiveID"
778         DataType="anyURI" />
779     </ActionMatch>
780 </Actions>
781 </Target>
782 <Rule RuleId="Consumer Data-Rate Allocation Objective Strategy
783 1" Effect="Permit">
784     <Condition FunctionId="and">
785         <Apply FunctionId="less-than-or-equal">
786             <SubjectAttributeDesignator DataType="integer"
787             AttributeId="fee" />
788             <AttributeValue DataType="integer">
789                 100
790             </AttributeValue>
791         </Apply>
792         <Apply FunctionId="greater-than-or-equal">
793             <ResourceAttributeDesignator DataType="integer"
794             AttributeId="data-rate" />
795             <AttributeValue DataType="integer">
796                 64000
797             </AttributeValue>
798         </Apply>
799     </Condition>
800 </Rule>
801 <Rule RuleId="Consumer Data-rate Allocation Objective Strategy
802 2" Effect="Permit">
803     <Condition FunctionId="and">
804         <Apply FunctionId="less-than-or-equal">
805             <SubjectAttributeDesignator DataType="integer"
806             AttributeId="fee" />
807             <AttributeValue DataType="integer">
808                 50
809             </AttributeValue>
810         </Apply>
811         <Apply FunctionId="greater-than-or-equal">
812             <ResourceAttributeDesignator DataType="integer"
813             AttributeId="data-rate" />
814             <AttributeValue DataType="integer">
815                 32000
816             </AttributeValue>
817         </Apply>
818         <Apply FunctionId="greater-than-or-equal">
819             <EnvironmentAttributeDesignator DataType="time"
820             AttributeId="timeOfDay" />
821             <AttributeValue DataType="time">
822                 21:00
823             </AttributeValue>
824         </Apply>
825     </Condition>
826 </Rule>
827 </Policy>
828 <</PolicySet>

```

829

Combining process

830

A.1.3. Combine <PolicySet> elements

831

The <Target> elements of the two <PolicySet> elements are identical. Therefore, they may

832

be combined. Append the provider <Policy> elements and assign a new PolicySetId value.

833

```

833 <PolicySet PolicySetId="Consumer Policy"
834 PolicyCombiningAlgId="deny-overrides">
835   <Target>
836     <Resources>
837       ResourceMatch MatchId="equal"
838         <AttributeValue DataType="anyURI">
839           serviceX:portX
840         </AttributeValue>
841       <ResourceAttributeDesignator AttributeId="portID"
842       DataType="anyURI" />
843     </ResourceMatch>
844   </Resources>
845   <Actions>
846     <AnyAction/>
847   </Actions>
848 </Target>
849 <Policy PolicyId="Consumer Data-rate Allocation Objective"
850       RuleCombiningAlgId="permit-overrides">
851   <Target>
852     <Actions>
853       <ActionMatch MatchId="equal">
854         <AttributeValue DataType="anyURI">
855           data-rate-allocation
856         </AttributeValue>
857         <ActionAttributeDesignator AttributeId="objectiveID"
858         DataType="anyURI" />
859       </ActionMatch>
860     </Actions>
861   </Target>
862   <Rule RuleId="Consumer Data-rate Allocation Objective Strategy
863   1" Effect="Permit">
864     <Condition FunctionId="and">
865       <Apply FunctionId="less-than-or-equal">
866         <SubjectAttributeDesignator DataType="integer"
867         AttributeId="fee" />
868         <AttributeValue DataType="integer">1.00</AttributeValue>
869       </Apply>
870       <Apply FunctionId="greater-than-or-equal">
871         <ResourceAttributeDesignator DataType="integer"
872         AttributeId="data-rate" />
873         <AttributeValue DataType="integer">
874           64000
875         </AttributeValue>
876       </Apply>
877     </Condition>
878   </Rule>
879   <Rule RuleId="Consumer Data-rate Allocation Objective Strategy
880   2" Effect="Permit">
881     <Condition FunctionId="and">

```



```

882         <Apply FunctionId="less-than-or-equal">
883             <SubjectAttributeDesignator DataType="integer"
884 AttributeId="fee"/>
885             <AttributeValue DataType="integer">0.50</AttributeValue>
886         </Apply>
887         <Apply FunctionId="greater-than-or-equal">
888             <ResourceAttributeDesignator DataType="integer"
889 AttributeId="data-rate"/>
890             <AttributeValue DataType="integer">
891                 32000
892             </AttributeValue>
893         </Apply>
894         <Apply FunctionId="greater-than-or-equal">
895             <EnvironmentAttributeDesignator DataType="time"
896 AttributeId="timeOfDay"/>
897             <AttributeValue DataType="time">9:00</AttributeValue>
898         </Apply>
899     </Condition>
900 </Rule>
901 </Policy>
902 <Policy PolicyId="Provider Data-rate Allocation Objective"
903     RuleCombiningAlgId="permit-overrides">
904     <Target>
905         <Actions>
906             <ActionMatch MatchId="equal">
907                 <AttributeValue DataType="anyURI">
908                     data-rate-allocation
909                 </AttributeValue>
910                 <ActionAttributeDesignator AttributeId="objectiveID"
911 DataType="anyURI"/>
912             </ActionMatch>
913         </Actions>
914     </Target>
915     <Rule RuleId="Provider Data-rate Allocation Objective Strategy
916 1" Effect="Permit">
917         <Condition FunctionId="and">
918             <Apply FunctionId="equal">
919                 <SubjectAttributeDesignator DataType="integer"
920 AttributeId="fee"/>
921                 <AttributeValue DataType="integer">1.50</AttributeValue>
922             </Apply>
923             <Apply FunctionId="greater-than-or-equal">
924                 <ResourceAttributeDesignator DataType="integer"
925 AttributeId="data-rate"/>
926                 <AttributeValue DataType="integer">
927                     64000
928                 </AttributeValue>
929             </Apply>
930         </Condition>
931     </Rule>
932     <Rule RuleId="Provider Data-rate Allocation Objective Strategy
933 2" Effect="Permit">
934         <Condition FunctionId="and">
935             <Apply FunctionId="equal">
936                 <SubjectAttributeDesignator DataType="integer"
937 AttributeId="fee"/>
938                 <AttributeValue DataType="integer">0.45</AttributeValue>
939             </Apply>
940             <Apply FunctionId="equal">

```

```

941         <ResourceAttributeDesignator DataType="integer"
942 AttributeId="data-rate"/>
943         <AttributeValue DataType="integer">
944             40000
945         </AttributeValue>
946     </Apply>
947     <Apply FunctionId="greater-than-or-equal">
948         <EnvironmentAttributeDesignator DataType="time"
949 AttributeId="timeOfDay"/>
950         <AttributeValue DataType="time">6:00</AttributeValue>
951     </Apply>
952 </Condition>
953 </Rule>
954 </Policy>
955 </PolicySet>

```

956 A.1.4. Combine <Policy> elements

957 The <Target> elements of the two <Policy> elements are identical. Therefore, they may be
958 combined. Append the provider <Rule> elements and assign a new PolicyId value.

```

959 <PolicySet PolicySetId="Combined Policies"
960 PolicyCombiningAlgId="deny-overrides">
961     <Target>
962         <Resources>
963             <ResourceMatch MatchId="equal"
964                 <AttributeValue DataType="anyURI">
965                     serviceX:portX
966                 </AttributeValue>
967                 <ResourceAttributeDesignator AttributeId="portID"
968 DataType="anyURI" />
969             </ResourceMatch>
970         </Resources>
971         <Actions>
972             <AnyAction/>
973         </Actions>
974     </Target>
975     <Policy PolicyId="Combined Data-rate Allocation Objective"
976         RuleCombiningAlgId="permit-overrides">
977         <Target>
978             <Actions>
979                 <ActionMatch MatchId="equal">
980                     <AttributeValue DataType="anyURI">
981                         data-rate-allocation
982                     </AttributeValue>
983                     <ActionAttributeDesignator AttributeId="objectiveID"
984 DataType="anyURI" />
985                 </ActionMatch>
986             </Actions>
987         </Target>
988         <Rule RuleId="Consumer Data-rate Allocation Objective Strategy
989 1" Effect="Permit">
990             <Condition FunctionId="and">
991                 <Apply FunctionId="less-than-or-equal">
992                     <SubjectAttributeDesignator DataType="integer"
993 AttributeId="fee" />
994                     <AttributeValue DataType="integer">1.00</AttributeValue>

```

```

995         </Apply>
996         <Apply FunctionId="greater-than-or-equal">
997             <ResourceAttributeDesignator DataType="integer"
998 AttributeId="data-rate"/>
999             <AttributeValue DataType="integer">
1000                 64000
1001             </AttributeValue>
1002         </Apply>
1003     </Condition>
1004 </Rule>
1005 <Rule RuleId="Consumer Data-rate Allocation Objective Strategy
1006 2" Effect="Permit">
1007     <Condition FunctionId="and">
1008         <Apply FunctionId="less-than-or-equal">
1009             <SubjectAttributeDesignator DataType="integer"
1010 AttributeId="fee"/>
1011             <AttributeValue DataType="integer">0.50</AttributeValue>
1012         </Apply>
1013         <Apply FunctionId="greater-than-or-equal">
1014             <ResourceAttributeDesignator DataType="integer"
1015 AttributeId="data-rate"/>
1016             <AttributeValue
1017 DataType="integer">32000</AttributeValue>
1018         </Apply>
1019         <Apply FunctionId="greater-than-or-equal">
1020             <EnvironmentAttributeDesignator DataType="time"
1021 AttributeId="timeOfDay"/>
1022             <AttributeValue DataType="time">9:00</AttributeValue>
1023         </Apply>
1024     </Condition>
1025 </Rule>
1026 <Rule RuleId="Provider Data-rate Allocation Objective Strategy
1027 1" Effect="Permit">
1028     <Condition FunctionId="and">
1029         <Apply FunctionId="equal">
1030             <SubjectAttributeDesignator DataType="integer"
1031 AttributeId="fee"/>
1032             <AttributeValue DataType="integer">1.50</AttributeValue>
1033         </Apply>
1034         <Apply FunctionId="greater-than-or-equal">
1035             <ResourceAttributeDesignator DataType="integer"
1036 AttributeId="data-rate"/>
1037             <AttributeValue DataType="integer">
1038                 64000
1039             </AttributeValue>
1040         </Apply>
1041     </Condition>
1042 </Rule>
1043 <Rule RuleId="Provider Data-rate Allocation Objective Strategy
1044 2" Effect="Permit">
1045     <Condition FunctionId="and">
1046         <Apply FunctionId="equal">
1047             <SubjectAttributeDesignator DataType="integer"
1048 AttributeId="fee"/>
1049             <AttributeValue DataType="integer">0.45</AttributeValue>
1050         </Apply>
1051         <Apply FunctionId="equal">
1052             <ResourceAttributeDesignator DataType="integer"
1053 AttributeId="data-rate"/>

```

```

1054         <AttributeValue DataType="integer">
1055             40000
1056         </AttributeValue>
1057     </Apply>
1058     <Apply FunctionId="greater-than-or-equal">
1059         <EnvironmentAttributeDesignator DataType="time"
1060 AttributeId="timeOfDay"/>
1061         <AttributeValue DataType="time">6:00</AttributeValue>
1062     </Apply>
1063 </Condition>
1064 </Rule>
1065 </Policy>
1066 </PolicySet>

```

1067 A.1.5. Combine <Rule> elements

1068 **Coincident** pairs of <Rule> elements are identified and combined. **Coincident** pairs of <Rule>
1069 elements are combined by appending the provider's <Apply> elements. Pairs are combined
1070 only where each member of the pair originally came from different <PolicySet> elements.

```

1071 <PolicySet PolicySetId="Combined Policies"
1072 PolicyCombiningAlgId="deny-overrides">
1073     <Target>
1074         <Resources>
1075             <ResourceMatch MatchId="equal"
1076                 <AttributeValue DataType="anyURI">
1077                     serviceX:portX
1078                 </AttributeValue>
1079                 <ResourceAttributeDesignator AttributeId="portID"
1080 DataType="anyURI"/>
1081             </ResourceMatch>
1082         </Resources>
1083         <Actions>
1084             <AnyAction/>
1085         </Actions>
1086     </Target>
1087     <Policy PolicyId="Combined Data-rate Allocation Objective"
1088 RuleCombiningAlgId="permit-overrides">
1089         <Target>
1090             <Actions>
1091                 <ActionMatch MatchId="equal">
1092                     <AttributeValue DataType="anyURI">
1093                         data-rate-allocation
1094                     </AttributeValue>
1095                     <ActionAttributeDesignator AttributeId="objectiveID"
1096 DataType="anyURI"/>
1097                 </ActionMatch>
1098             </Actions>
1099         </Target>
1100         <Rule RuleId="Consumer Strategy 1/Provider Strategy 1"
1101 Effect="Permit">
1102             <Condition FunctionId="and">
1103                 <Apply FunctionId="less-than-or-equal">
1104                     <SubjectAttributeDesignator DataType="integer"
1105 AttributeId="fee"/>
1106                     <AttributeValue DataType="integer">1.00</AttributeValue>
1107                 </Apply>

```

```

1108         <Apply FunctionId="greater-than-or-equal">
1109             <ResourceAttributeDesignator DataType="integer"
1110 AttributeId="data-rate"/>
1111             <AttributeValue DataType="integer">
1112                 64000
1113             </AttributeValue>
1114         </Apply>
1115         <Apply FunctionId="equal">
1116             <SubjectAttributeDesignator DataType="integer"
1117 AttributeId="fee"/>
1118             <AttributeValue DataType="integer">1.50</AttributeValue>
1119         </Apply>
1120         <Apply FunctionId="greater-than-or-equal">
1121             <ResourceAttributeDesignator DataType="integer"
1122 AttributeId="data-rate"/>
1123             <AttributeValue DataType="integer">
1124                 64000
1125             </AttributeValue>
1126         </Apply>
1127     </Condition>
1128 </Rule>
1129 <Rule RuleId="Consumer Strategy 1/Provider Strategy 2"
1130 Effect="Permit">
1131     <Condition FunctionId="and">
1132         <Apply FunctionId="less-than-or-equal">
1133             <SubjectAttributeDesignator DataType="integer"
1134 AttributeId="fee"/>
1135             <AttributeValue DataType="integer">1.00</AttributeValue>
1136         </Apply>
1137         <Apply FunctionId="greater-than-or-equal">
1138             <ResourceAttributeDesignator DataType="integer"
1139 AttributeId="data-rate"/>
1140             <AttributeValue DataType="integer">64000</AttributeValue>
1141         </Apply>
1142         <Apply FunctionId="equal">
1143             <SubjectAttributeDesignator DataType="integer"
1144 AttributeId="fee"/>
1145             <AttributeValue DataType="integer">0.45</AttributeValue>
1146         </Apply>
1147         <Apply FunctionId="equal">
1148             <ResourceAttributeDesignator DataType="integer"
1149 AttributeId="data-rate"/>
1150             <AttributeValue DataType="integer">40000</AttributeValue>
1151         </Apply>
1152         <Apply FunctionId="greater-than-or-equal">
1153             <EnvironmentAttributeDesignator DataType="time"
1154 AttributeId="timeOfDay"/>
1155             <AttributeValue DataType="time">6:00</AttributeValue>
1156         </Apply>
1157     </Condition>
1158 </Rule>
1159 <Rule RuleId="Consumer Strategy 2/Provider Strategy 1"
1160 Effect="Permit">
1161     <Condition FunctionId="and">
1162         <Apply FunctionId="less-than-or-equal">
1163             <SubjectAttributeDesignator DataType="integer"
1164 AttributeId="fee"/>
1165             <AttributeValue DataType="integer">0.50</AttributeValue>
1166         </Apply>

```

```

1167         <Apply FunctionId="greater-than-or-equal">
1168             <ResourceAttributeDesignator DataType="integer"
1169 AttributeId="data-rate"/>
1170             <AttributeValue DataType="integer">32000</AttributeValue>
1171         </Apply>
1172         <Apply FunctionId="greater-than-or-equal">
1173             <EnvironmentAttributeDesignator DataType="time"
1174 AttributeId="timeOfDay"/>
1175             <AttributeValue DataType="time">9:00</AttributeValue>
1176         </Apply>
1177         <Apply FunctionId="equal">
1178             <SubjectAttributeDesignator DataType="integer"
1179 AttributeId="fee"/>
1180             <AttributeValue DataType="integer">1.50</AttributeValue>
1181         </Apply>
1182         <Apply FunctionId="greater-than-or-equal">
1183             <ResourceAttributeDesignator DataType="integer"
1184 AttributeId="data-rate"/>
1185             <AttributeValue DataType="integer">64000</AttributeValue>
1186         </Apply>
1187     </Condition>
1188 </Rule>
1189 <Rule RuleId="Consumer Strategy 2/Provider Strategy 2"
1190 Effect="Permit">
1191     <Condition FunctionId="and">
1192         <Apply FunctionId="less-than-or-equal">
1193             <SubjectAttributeDesignator DataType="integer"
1194 AttributeId="fee"/>
1195             <AttributeValue DataType="integer">0.50</AttributeValue>
1196         </Apply>
1197         <Apply FunctionId="greater-than-or-equal">
1198             <ResourceAttributeDesignator DataType="integer"
1199 AttributeId="data-rate"/>
1200             <AttributeValue DataType="integer">32000</AttributeValue>
1201         </Apply>
1202         <Apply FunctionId="greater-than-or-equal">
1203             <EnvironmentAttributeDesignator DataType="time"
1204 AttributeId="timeOfDay"/>
1205             <AttributeValue DataType="time">9:00</AttributeValue>
1206         </Apply>
1207         <Apply FunctionId="equal">
1208             <SubjectAttributeDesignator DataType="integer"
1209 AttributeId="fee"/>
1210             <AttributeValue DataType="integer">0.45</AttributeValue>
1211         </Apply>
1212         <Apply FunctionId="equal">
1213             <ResourceAttributeDesignator DataType="integer"
1214 AttributeId="data-rate"/>
1215             <AttributeValue DataType="integer">40000</AttributeValue>
1216         </Apply>
1217         <Apply FunctionId="greater-than-or-equal">
1218             <EnvironmentAttributeDesignator DataType="time"
1219 AttributeId="timeOfDay"/>
1220             <AttributeValue DataType="time">6:00</AttributeValue>
1221         </Apply>
1222     </Condition>
1223 </Rule>
1224 </Policy>
1225 </PolicySet>

```

1226 A.1.6. Combine <Apply> elements

1227 <Apply> elements are combined if they are combinable according to Table 1.

```
1228 <PolicySet PolicySetId="Combined Policies"  
1229 PolicyCombiningAlgId="deny-overrides">  
1230   <Target>  
1231     <Resources>  
1232       <ResourceMatch MatchId="equal"  
1233         <AttributeValue DataType="anyURI">  
1234           serviceX:portX  
1235         </AttributeValue>  
1236         <ResourceAttributeDesignator AttributeId="portID"  
1237         DataType="anyURI" />  
1238       </ResourceMatch>  
1239     </Resources>  
1240     <Actions>  
1241       <AnyAction/>  
1242     </Actions>  
1243   </Target>  
1244   <Policy PolicyId="Combined Data-rate Allocation Objective"  
1245     RuleCombiningAlgId="permit-overrides">  
1246     <Target>  
1247       <Actions>  
1248         <ActionMatch MatchId="equal">  
1249           <AttributeValue DataType="anyURI">data-rate-  
1250 allocation</AttributeValue>  
1251           <ActionAttributeDesignator AttributeId="objectiveID"  
1252           DataType="anyURI" />  
1253         </ActionMatch>  
1254       </Actions>  
1255     </Target>  
1256     <!-- Rule RuleId="Consumer Strategy 1/Provider Strategy 2"  
1257     Effect="Permit"  
1258       Fee predicates are incompatible -->  
1259     <!-- Rule RuleId="Consumer Strategy 1/Provider Strategy 2"  
1260     Effect="Permit"  
1261       Data-rate predicates are incompatible -->  
1262     <!-- Rule RuleId="Consumer Strategy 2/Provider Strategy 1"  
1263     Effect="Permit"  
1264       Fee predicates are incompatible -->  
1265     <Rule RuleId="Consumer Strategy 2/Provider Strategy 2"  
1266     Effect="Permit">  
1267       <Condition FunctionId="and">  
1268         <Apply FunctionId="equal">  
1269           <SubjectAttributeDesignator DataType="integer"  
1270           AttributeId="fee" />  
1271           <AttributeValue DataType="integer">0.45</AttributeValue>  
1272         </Apply>  
1273         <Apply FunctionId="equal">  
1274           <ResourceAttributeDesignator DataType="integer"  
1275           AttributeId="data-rate" />  
1276           <AttributeValue DataType="integer">  
1277             40000  
1278           </AttributeValue>  
1279         </Apply>  
1280       <Apply FunctionId="greater-than-or-equal">
```

```

1281         <EnvironmentAttributeDesignator DataType="time"
1282 AttributeId="timeOfDay" />
1283         <AttributeValue DataType="time">9:00</AttributeValue>
1284     </Apply>
1285 </Condition>
1286 </Rule>
1287 </Policy>
1288 </PolicySet>

```

1289 A.1.7. Substitute <Apply> elements

1290 Elimination is achieved by deleting all except the first <Rule> element.

```

1291 <PolicySet PolicySetId="Combined Policies"
1292 PolicyCombiningAlgId="deny-overrides">
1293   <Target>
1294     <Resources>
1295       <ResourceMatch MatchId="equal"
1296         <AttributeValue DataType="anyURI">
1297           serviceX:portX
1298         </AttributeValue>
1299         <ResourceAttributeDesignator AttributeId="portID"
1300 DataType="anyURI" />
1301       </ResourceMatch>
1302     </Resources>
1303     <Actions>
1304       <AnyAction />
1305     </Actions>
1306   </Target>
1307   <Policy PolicyId="Combined Data-rate Allocation Objective"
1308     RuleCombiningAlgId="permit-overrides">
1309     <Target>
1310       <Actions>
1311         <ActionMatch MatchId="equal">
1312           <AttributeValue DataType="anyURI">
1313             data-rate-allocation
1314           </AttributeValue>
1315           <ActionAttributeDesignator AttributeId="objectiveID"
1316 DataType="anyURI" />
1317         </ActionMatch>
1318       </Actions>
1319     </Target>
1320     <Rule RuleId="Consumer Strategy 2/Provider Strategy 2"
1321 Effect="Permit">
1322       <Condition FunctionId="and">
1323         <Apply FunctionId="equal">
1324           <SubjectAttributeDesignator DataType="integer"
1325 AttributeId="fee" />
1326           <AttributeValue DataType="integer">0.45</AttributeValue>
1327         </Apply>
1328         <Apply FunctionId="equal">
1329           <ResourceAttributeDesignator DataType="integer"
1330 AttributeId="data-rate" />
1331           <AttributeValue DataType="integer">
1332             40000
1333           </AttributeValue>
1334         </Apply>

```



```
1335         <Apply FunctionId="equal">
1336             <EnvironmentAttributeDesignator DataType="time"
1337 AttributeId="timeOfDay" />
1338             <AttributeValue DataType="time">9:00</AttributeValue>
1339         </Apply>
1340     </Condition>
1341 </Rule>
1342 </Policy>
1343 </PolicySet>
```

Appendix B. Revision history

Rev	Date	By whom	What
Draft 02	23 July 2003	Tim Moses	<p>Limited functions and data-types to those defined by XACML.</p> <p>Prohibited the nesting of <Apply> elements.</p> <p>In the WSDL binding, targeted top-level policy statements at <wsdl:port> elements.</p> <p>Introduced two levels of <PolicySet> elements to allow finer targeting of policy statements.</p> <p>Added a "Security Considerations" section.</p> <p>Introduced the elimination step.</p>

Appendix C. Notices

1346

1347 OASIS takes no position regarding the validity or scope of any intellectual property or other rights
1348 that might be claimed to pertain to the implementation or use of the technology described in this
1349 document or the extent to which any license under such rights might or might not be available;
1350 neither does it represent that it has made any effort to identify any such rights. Information on
1351 OASIS's procedures with respect to rights in OASIS specifications can be found at the OASIS
1352 website. Copies of claims of rights made available for publication and any assurances of licenses
1353 to be made available, or the result of an attempt made to obtain a general license or permission
1354 for the use of such proprietary rights by implementors or users of this specification, can be
1355 obtained from the OASIS Executive Director.

1356 OASIS has been notified of intellectual property rights claimed in regard to some or all of the
1357 contents of this specification. For more information consult the online list of claimed rights.

1358 OASIS invites any interested party to bring to its attention any copyrights, patents or patent
1359 applications, or other proprietary rights which may cover technology that may be required to
1360 implement this specification. Please address the information to the OASIS Executive Director.

1361 Copyright (C) OASIS Open 2003. All Rights Reserved.

1362 This document and translations of it may be copied and furnished to others, and derivative works
1363 that comment on or otherwise explain it or assist in its implementation may be prepared, copied,
1364 published and distributed, in whole or in part, without restriction of any kind, provided that the
1365 above copyright notice and this paragraph are included on all such copies and derivative works.
1366 However, this document itself may not be modified in any way, such as by removing the copyright
1367 notice or references to OASIS, except as needed for the purpose of developing OASIS
1368 specifications, in which case the procedures for copyrights defined in the OASIS Intellectual
1369 Property Rights document must be followed, or as required to translate it into languages other
1370 than English.

1371 The limited permissions granted above are perpetual and will not be revoked by OASIS or its
1372 successors or assigns.

1373 This document and the information contained herein is provided on an "AS IS" basis and OASIS
1374 DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO
1375 ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE
1376 ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A
1377 PARTICULAR PURPOSE.