



XACML 3.0 Export Compliance-US (EC-US) Profile Version 1.0

Committee Draft 02

24 September 2009

Specification URIs:

This Version:

<http://docs.oasis-open.org/xacml/3.0/xacml-3.0-ec-us-v1-spec-cd-02-en.html>
<http://docs.oasis-open.org/xacml/3.0/xacml-3.0-ec-us-v1-spec-cd-02-en.doc> (Authoritative)
<http://docs.oasis-open.org/xacml/3.0/xacml-3.0-ec-us-v1-spec-cd-02-en.pdf>

Previous Version:

N/A

Latest Version:

<http://docs.oasis-open.org/xacml/3.0/xacml-3.0-ec-us-v1-spec-en.html>
<http://docs.oasis-open.org/xacml/3.0/xacml-3.0-ec-us-v1-spec-en.doc>
<http://docs.oasis-open.org/xacml/3.0/xacml-3.0-ec-us-v1-spec-en.pdf>

Technical Committee:

[OASIS eXtensible Access Control Markup Language \(XACML\) TC](#)

Chair(s):

Bill Parducci, <bill@parducci.net>
Hal Lockhart, Oracle <hal.lockhart@oracle.com>

Editor(s):

John Tolbert, The Boeing Company

Related work:

This specification is related to:

- [eXtensible Access Control Markup Language \(XACML\)](#)

Abstract:

This specification defines a profile for the use of XACML in expressing policies for complying with USA government regulations for export compliance (EC). It defines standard attribute identifiers useful in such policies, and recommends attribute value ranges for certain attributes.

Status:

This document was last revised or approved by the eXtensible Access Control Markup Language (XACML) 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/xacml/>.

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/xacml/ipr.php>).

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

Notices

Copyright © OASIS® 2009. 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", [insert specific trademarked names and abbreviations here] 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.....	5
1.1	Glossary.....	5
1.2	Terminology.....	6
1.3	Normative References.....	6
1.4	Non-Normative References.....	6
1.5	Scope.....	6
1.6	Disclaimer.....	6
2	Profile.....	7
2.1	Resource Attributes.....	7
2.1.1	Classification.....	7
2.1.1	ECCN.....	7
2.1.2	USML.....	7
2.2	Subject Attributes.....	7
2.2.1	Nationality.....	7
2.2.2	Current nationality.....	8
2.2.3	Location.....	8
2.2.4	Organization.....	8
2.2.5	US Person.....	8
3	Identifiers.....	9
3.1	Profile Identifier.....	9
4	Examples (non-normative).....	10
4.1	Commerce Control List rule.....	10
4.2	State Department agreement.....	11
5	Conformance.....	14
5.1	Attribute Identifiers.....	14
5.2	Attribute Values.....	14
A.	Acknowledgements.....	15
B.	Non-Normative Text.....	Error! Bookmark not defined.
C.	Revision History.....	16

1 Introduction

{non-normative}

This specification defines a profile for the use of the OASIS eXtensible Access Control Markup Language (XACML) [XACML] to write policies that reflect the intent of United States government, particularly the Department of Commerce export compliance (EC) laws and regulations. Use of this profile requires no changes or extensions to the [XACML] standard.

This specification begins with a non-normative discussion of the topics of interest in this profile. The normative section of the specification describes the attributes defined by this profile and provides recommended usage patterns for attribute values.

This specification assumes the reader is somewhat familiar with XACML. A brief overview sufficient to understand these examples is available in [XACMLIntro]. Information about USA government export laws and regulations can be found at [BIS] and [DDTC].

Any U.S. organization that ships goods, materials, software, and/or technical information may be subject to U.S. export control laws. Non-military products may be classified according to the U.S. Department of Commerce "Commerce Control List". Military products are controlled according to the United States Munitions List. Destination countries are also classified by a variety of criteria. Even specific entities and individuals may have restrictions. The recipient's U.S. person status, location, and organization must also be taken into account in these export control authorization decisions.

This EC-US profile provides a standard framework for the subject and resource attributes that must be considered for U.S. export control decisions.

1.1 Glossary

CCL, Commerce Control List

Regulations that define the geopolitical restrictions on goods and services covered by *EAR*.

Country

A national political administrative unit recognized, for diplomatic and trade purposes, by the US government.

Current nationality

For any person, the *current nationality* is the *country* that most recently granted citizenship to that person.

EAR

Export Administration Regulations, US laws and regulations administered by the Department of Commerce.

ECCN

Export Control Classification Number, a classification system for data and products covered by *EAR*.

ITAR

International Traffic in Arms Regulations; USA laws and regulations administered by the Department of State.

Location

The *country* in which a person is currently located.

Nationality

A country of which a person is a citizen.

Organization

44 A company or other legal entity of which a person can be an employee or agent.

45 **USML**

46 United States Munitions List, a classification system for data and products covered by **ITAR**.

47 **US Person**

48 A designation that a person meets the requirements to be considered exempt from most US government
49 export regulations.

50 **1.2 Terminology**

51 The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD
52 NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described
53 in **[RFC2119]**.

54 **1.3 Normative References**

55 **[RFC2119]** S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*,
56 <http://www.ietf.org/rfc/rfc2119.txt>, IETF RFC 2119, March 1997.

57 **[XACML]** OASIS, Committee Draft 02, 3 November 2008, *eXtensible Access Control*
58 *Markup Language (XACML) Version 3.0*, [http://www.oasis-](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml)
59 [open.org/committees/tc_home.php?wg_abbrev=xacml](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml)

60 **1.4 Non-Normative References**

61 **[BIS]** US Department of Commerce Bureau of Industry and Security,
62 <http://www.bis.doc.gov/>

63 **[DDTC]** US Department of State Directorate of Defense Trade Controls,
64 <http://www.pmdtc.state.gov/>

65 **[ISO3166]** ISO 3166 Maintenance agency (ISO 3166/MA),
66 http://www.iso.org/iso/country_codes.htm

67 **[XACMLIntro]** OASIS XACML TC, *A Brief Introduction to XACML*, 14 March 2003,
68 [http://www.oasis-](http://www.oasis-open.org/committees/download.php/2713/Brief_Introduction_to_XACML.html)
69 [open.org/committees/download.php/2713/Brief_Introduction_to_XACML.html](http://www.oasis-open.org/committees/download.php/2713/Brief_Introduction_to_XACML.html)

70 **1.5 Scope**

71 Many export compliance decisions can be made on the basis of the subject’s **location**, **organization**, and
72 **nationalities** (including country of birth) or **current nationality**, and the resource’s **ECCN** or **USML**
73 classification. This profile defines standard XACML attributes for these properties, and recommends the
74 use of standardized attribute values.

75 In practice, an organization’s export compliance policies will be a mixture of rules derived from US
76 government laws and regulations, along with enterprise-specific rules derived from government-approved
77 bilateral or multilateral agreements with foreign organizations.

78 **1.6 Disclaimer**

79 NOTHING IN THIS PROFILE IS INTENDED TO BE A LEGALLY CORRECT INTERPRETATION OR
80 APPLICATION OF US GOVERNMENT EXPORT LAWS OR REGULATIONS. USE OF THIS PROFILE IN
81 AN ACCESS CONTROL SYSTEM DOES NOT CONSTITUTE COMPLIANCE WITH US EXPORT
82 RESTRICTIONS. THIS PROFILE HAS NOT BEEN REVIEWED OR ENDORSED BY THE US
83 GOVERNMENT AGENCIES RESPONSIBLE FOR ENFORCING USA EXPORT LAWS, NOR BY ANY
84 LEGAL EXPERT IN THIS FIELD.

85 Organizations that use this profile should ensure their export compliance by consulting the resources at
86 **[BIS]** and **[DDTC]**, and by engaging qualified professional legal services.

87 2 Profile

88 2.1 Resource Attributes

89 2.1.1 Classification

90 To identify whether a resource is controlled under **[ITAR]** or **[EAR]**, the following attribute identifier shall
91 be used:

92 `urn:oasis:names:tc:xacml:3.0:ec-us:resource:classification`

93 The `DataType` of this attribute is `http://www.w3.org/2001/XMLSchema#string`. The value of the
94 attribute SHALL be "ITAR" or "EAR".

95 2.1.1 ECCN

96 ECCN classification values shall be designated with the following attribute identifier:

97 `urn:oasis:names:tc:xacml:3.0:ec-us:resource:eccn`

98 The attribute value (or pattern) used in equality or matching comparisons (in **policies**), and the attribute
99 values used in the **decision context** SHALL conform to the following requirements:

- 100 • The base ECCN classification shall be 5 characters with upper-case letters.

101 `9A120`

- 102 • Subclassification levels may be used, corresponding to the subparagraph labels in the **CCL**. The
103 subclassification designators shall be delimited with dots (".").

104 `3A001.b.1.a.4.c`

- 105 • All comparisons shall be case-sensitive.

106 2.1.2 USML

107 USML classification values shall be designated with the following attribute identifier:

108 `urn:oasis:names:tc:xacml:3.0:ec-us:resource:usml`

109 The attribute value (or pattern) used in equality or matching comparisons (in **policies**), and the attribute
110 values used in the **decision context** SHALL conform to the following requirements:

- 111 • The minimal value (or pattern) shall consist of an upper-case roman numeral (in the range specified
112 by the **USML**), followed by a balanced set of parentheses containing a single lower-case letter.

113 `VIII(i)`

- 114 • Additional balanced parentheses may be appended to the minimal value (or pattern), corresponding
115 to subparagraph designations in the **USML**.

116 `V(b)(7)(c)(2)`

- 117 • All comparisons shall be case-sensitive.

118 2.2 Subject Attributes

119 2.2.1 Nationality

120 Nationality values applicable to a subject SHALL be designated with the following attribute identifier:

121 `urn:oasis:names:tc:xacml:3.0:ec-us:subject:nationality`

122 The `DataType` of this attribute is `http://www.w3.org/2001/XMLSchema#string`. The value of this
123 attribute MUST be in the range of 2-letter country codes defined by **[ISO3166]**.

124 A request context may have several instances of this attribute to reflect multiple citizenships held by a
125 subject. Nationality must include country of birth if different from other nationalities held by the subject.

126 2.2.2 Current nationality

127 The most recent nationality value applicable to a subject SHALL be designated with the following attribute
128 identifier:

129 `urn:oasis:names:tc:xacml:3.0:ec-us:subject:current-nationality`

130 The `DataType` of this attribute is `http://www.w3.org/2001/XMLSchema#string`. The value of this
131 attribute MUST be in the range of 2-letter country codes defined by **[ISO3166]**.

132 2.2.3 Location

133 The current geographical location of a subject SHALL be designated with the following attribute identifier:

134 `urn:oasis:names:tc:xacml:3.0:ec-us:subject:location`

135 The `DataType` of this attribute is `http://www.w3.org/2001/XMLSchema#string`. The value of this
136 attribute MUST be in the range of 2-letter country codes defined by **[ISO3166]**.

137 2.2.4 Organization

138 The organization of which the subject is an employee or agent SHALL be designated with the following
139 attribute identifier:

140 `urn:oasis:names:tc:xacml:3.0:ec-us:subject:organization`

141 Organization shall denote the organization to which the subject in the request belongs. A common
142 scheme such as DUNS SHOULD be used to promote interoperability.

143 2.2.5 US Person

144 The following attribute identifier SHALL be used to designate a subject's status as a **US person**:

145 `urn:oasis:names:tc:xacml:3.0:ec-us:subject:us-person`

146 The `DataType` of this attribute is `http://www.w3.org/2001/XMLSchema#boolean`.

147 **3 Identifiers**

148 This profile defines the following URN identifiers.

149 **3.1 Profile Identifier**

150 The following identifier SHALL be used as the identifier for this profile when an identifier in the form of a
151 URI is required.

152 `urn:oasis:names:tc:xacml:3.0:profiles:ec-us`

153

154 4 Examples (non-normative)

155 This section contains two examples illustrating the use of the attribute IDs defined by this profile.

156 The following entity definitions are used in these examples

```
157 <!ENTITY ec-us-subj "urn:oasis:names:tc:xacml:3.0:ec-us:subject:">
158 <!ENTITY ec-us-res "urn:oasis:names:tc:xacml:3.0:ec-us:resource:">
159 <!ENTITY func10 "urn:oasis:names:tc:xacml:1.0:function:">
160 <!ENTITY resource_category
161 "urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
162 <!ENTITY subject_category
163 "urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
164 <!ENTITY xacml-res "urn:oasis:names:tc:xacml:1.0:resource:">
165 <!ENTITY xs "http://www.w3.org/2001/XMLSchema#">
```

166 Some required attributes, not essential for understanding, are omitted from the examples.

167 4.1 Commerce Control List rule

168 This illustrates one way to implement a rule for an **ECCN** as defined in the **CCL**. In English

169 *Deny access to persons and locations in the anti-terrorism (AT1) and non-proliferation (NP1) country lists*
170 *if the resource has **ECCN** starting with "3A980".*

```
171 [a1] <?xml version="1.0" encoding="UTF-8"?>
172 [a2] <Policy
173 [a3]     xmlns="urn:oasis:names:tc:xacml:3.0:schema:os"
174 [a4]     PolicyId="urn:oasis:names:tc:xacml:3.0:ec-us:example:CCL"
175 [a5]     Version="1.0"
176 [a6]     RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-
177 algorithm:first-applicable ">
178 [a7]   <Description>
179 [a8]     Simple rule for one ECCN.
180 [a9]   </Description>
181 [a10]  <Target/>
182 [a11]  <VariableDefinition VariableId="AT1">
183 [a12]    <!-- Anti-terrorism -->
184 [a13]    <Apply FunctionId="&func10;any-of-any">
185 [a14]      <Function FunctionId="&func10:string-equal"/>
186 [a15]      <Apply FunctionId="&func10:string-union">
187 [a16]        <AttributeDesignator
188 [a17]          Category="&subject_category;"
189 [a18]          AttributeId="&ec-us-subj;current-nationality"/>
190 [a19]        <AttributeDesignator
191 [a20]          Category="&subject_category;"
192 [a21]          AttributeId="&ec-us-subj;location"/>
193 [a22]      </Apply>
194 [a23]    <Apply FunctionId="&func10:string-bag">
195 [a24]      <AttributeValue DataType="&xs:string">SD</AttributeValue>
196 [a25]      <AttributeValue DataType="&xs:string">SY</AttributeValue>
197 [a26]    </Apply>
198 [a27]  </VariableDefinition>
199 [a28]  <VariableDefinition VariableId="NP1">
200 [a29]    <!-- similar to AT1 -->
201 [a30]  </VariableDefinition>
202 [a31]  <Rule RuleId="3A980" Effect="Deny">
203 [a32]    <Description>
204 [a33]      Voice print identification and analysis equipment and parts...
205 [a34]    </Description>
206 [a35]  <Target>
207 [a36]    <AnyOf>
208 [a37]
```

```

209 [a38]         <AllOf>
210 [a39]             <Match MatchId="&func10;string-regexp-match">
211 [a40]                 <AttributeValue
212 [a41]                     DataType="&xs:string">^3A980.*</AttributeValue>
213 [a42]                 <AttributeDesignator Category="&resource_category;"
214 [a43]                     AttributeId="&ec-us-res;eccn"/>
215 [a44]             </Match>
216 [a45]         </AllOf>
217 [a46]     </AnyOf>
218 [a47] </Target>
219 [a48] <Condition>
220 [a49]     <Apply FunctionId="&func10;or">
221 [a50]         <VariableReference VariableId="AT1"/>
222 [a51]         <VariableReference VariableId="NP2"/>
223 [a52]     </Apply>
224 [a53] </Condition>
225 [a54] </Rule>
226 [a55] </Policy>

```

227 [a11-a28] Define a variable that returns true if the subject's `current-nationality` or `location` is
228 "SD" or "SY". These are the countries listed under the anti-terrorism reason for control in the **CCL**.

229 [a29-a31] Define another variable to check if `current-nationality` or `location` is in the group of
230 countries controlled for nuclear non-proliferation.

231 NOTE: In a real policy, it would be convenient to define variables corresponding to each
232 "reason for control" in the CCL. This example only refers to 2 such variables.

233 [a32] Define a rule that applies to resources with an **ECCN** classification (`eccn`) of "3A980".

234 [a48-a53] Test if subject has a `current-nationality` or `location` that is controlled for this
235 classification.

236 NOTE: A real policy could have rules for every **ECCN** classification used in the enterprise
237 (or defined by **[BIS]**).

238 4.2 State Department agreement

239 This illustrates one way to write a XACML policy to implement an export authorization. In English:

240 *Employees of BrazilEnterprise and employees of CanadianEnterprise who have no other nationality*
241 *attributes than "CA" or BR" are permitted to view resources identified with an "EXP" suffix that are*
242 *classified as "ITAR" and have USML code "VIII(h)".*

243 The (fictional) authorizing document is a Technical Assistance Agreement (TAA) identified as "TA-XYZ-
244 00".

```

245 [b1]     <Policy PolicyId="TA-XYZ-00" RuleCombiningAlgorithmId="...">
246 [b2]         <Description>Permit exports to Canadian and Brazilian partners.
247 [b3]     </Description>
248 [b4]     <Target>
249 [b5]         <AnyOf>
250 [b6]             <AllOf>
251 [b7]                 <Match MatchId="&func10;string-regexp-match">
252 [b8]                     <AttributeValue DataType="&xs:string">EXP$</AttributeValue>
253 [b9]                     <AttributeDesignator Category="&resource_category;"
254 [b10]                         AttributeId="&xacml-res;resource-id"/>
255 [b11]                 </Match>
256 [b12]                 <Match MatchId="&func10;string-equal">
257 [b13]                     <AttributeValue DataType="&xs:string">ITAR</AttributeValue>
258 [b14]                     <AttributeDesignator Category="&resource_category;"
259 [b15]                         AttributeId="&ec-us-res;classification"/>
260 [b16]                 </Match>
261 [b17]             </AllOf>
262 [b18]         </AnyOf>
263 [b19]     </AnyOf>

```

```

264 [b20]      <-- Subject must work for a partner organization -->
265 [b21]      <AllOf>
266 [b22]          <Match MatchId="&func10;string-equal">
267 [b23]              <AttributeValue DataType="&xs:string">
268 [b24]                  BrazilEnterprise
269 [b25]              </AttributeValue>
270 [b26]              <AttributeDesignator Category="&subject_category;"
271 [b27]                  AttributeId="&ec-us-subj;organization" />
272 [b28]          </Match>
273 [b29]      </AllOf>
274 [b30]      <AllOf>
275 [b31]          <Match MatchId="&func10;string-equal">
276 [b32]              <AttributeValue DataType="&xs:string">
277 [b33]                  CanadianEnterprise
278 [b34]              </AttributeValue>
279 [b35]              <AttributeDesignator Category="&subject_category;"
280 [b36]                  AttributeId="&ec-us-subj;organization" />
281 [b37]          </Match>
282 [b38]      </AllOf>
283 [b39]      </AnyOf>
284 [b40]      </Target>
285 [b41]      <VariableDefinition VariableId="TA-XYZ-00-nationalities">
286 [b42]          <!-- Subject must hold no nationalities other than "BR", "CA"
287 [b43]          -->
288 [b44]          <Apply FunctionId="&func10;string-subset">
289 [b45]              <AttributeDesignator MustBePresent="false"
290 [b46]                  Category="&subject_category;"
291 [b47]                  AttributeId="&ec-us-subj;nationality"
292 [b48]                  DataType="&xs:string" />
293 [b49]              <Apply FunctionId="&func10;string-bag">
294 [b50]                  <AttributeValue DataType="&xs:string">BR</AttributeValue>
295 [b51]                  <AttributeValue DataType="&xs:string">CA</AttributeValue>
296 [b52]              </Apply>
297 [b53]          </Apply>
298 [b54]      </VariableDefinition>
299 [b55]      <Rule RuleId="permit-TA-XYZ-00" Effect="Permit">
300 [b56]          <Target>
301 [b57]              <AnyOf>
302 [b58]                  <AllOf>
303 [b59]                      <Match MatchId="&func10;string-equal">
304 [b60]                          <AttributeValue
305 [b61]                              DataType="&xs:string">VIII(h)</AttributeValue>
306 [b62]                          <AttributeDesignator Category="&resource_category;"
307 [b63]                              AttributeId="&ec-us-res;usml" />
308 [b64]                      </Match>
309 [b65]                  </AllOf>
310 [b66]              </AnyOf>
311 [b67]          </Target>
312 [b68]          <Condition>
313 [b69]              <VariableReference VariableId="TA-XYZ-00-nationalities" />
314 [b70]          </Condition>
315 [b71]      </Rule>
316 [b72]      </Policy>

```

317 [b5-b18] This policy applies to resources with resource-id ending in "EXP" that have
318 classification equal to "ITAR".

319 [b19-b39] This policy applies to subjects who work for (have organization attribute) of
320 "BrazilianEnterprise" or "CanadianEnterprise".

321 [b41-b54] Define a variable to test that all nationality values are in the set ("BR", "CA").

322 [b55-b71] Define a rule that permits access if the usml is "VIII(h)" and the subject's nationality values
323 are all in the specified set.

324
325

NOTE: For correct evaluation, the request context must contain the complete set of nationality values (including country of birth) for the subject.

326 5 Conformance

327 Conformance to this profile is defined for *policies* and *requests* generated and transmitted within and
328 between XACML systems.

329 5.1 Attribute Identifiers

330 Conformant XACML *policies* and *requests* SHALL use the attribute identifiers defined in Section 2 for
331 their specified purpose, and SHALL NOT use any other identifiers for the purposes defined by attributes
332 in this profile. The following table lists the attributes that must be supported.

333 Note: “M” is mandatory “O” is optional.

334

Identifiers	
urn:oasis:names:tc:xacml:3.0:ec-us:resource:eccn	M
urn:oasis:names:tc:xacml:3.0:ec-us:resource:usml	M
urn:oasis:names:tc:xacml:3.0:ec-us:subject:nationality	M
urn:oasis:names:tc:xacml:3.0:ec-us:subject:current-nationality	M
urn:oasis:names:tc:xacml:3.0:ec-us:subject:location	M
urn:oasis:names:tc:xacml:3.0:ec-us:subject:organization	M
urn:oasis:names:tc:xacml:3.0:ec-us:subject:us-person	M

335

336 5.2 Attribute Values

337 Conformant XACML *policies* and *requests* SHALL use attribute values in the specified range or patterns
338 as defined for each attribute in Section 2 (when a range or pattern is specified).

339 NOTE: In order to process conformant XACML *policies* and *requests* correctly, *PIP* and
340 *PEP* modules may have to translate native data values into the datatypes and formats
341 specified in this profile.

342 **A. Acknowledgements**

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

345 **Participants:**

346 John Tolbert, The Boeing Company
347 Paul Tyson, Associate

348

B. Revision History

349

Revision	Date	Editor	Changes Made
WD 1	4/17/2009	John Tolbert	Initial draft
WD 2	6/2/2009	John Tolbert	Added descriptions and conformance section
CD 1	7/2/2009	John Tolbert/Paul Tyson	Annotated examples
CD 2	9/2/2009	Paul Tyson	Add conformance table

350