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

Committee Specification Draft 05 / Public Review Draft 03

10 January 2013

Specification URIs

This version:

http://docs.oasis-open.org/xacml/3.0/ec-us/v1.0/csprd03/xacml-3.0-ec-us-v1.0-csprd03.doc (Authoritative)
http://docs.oasis-open.org/xacml/3.0/ec-us/v1.0/csprd03/xacml-3.0-ec-us-v1.0-csprd03.html
http://docs.oasis-open.org/xacml/3.0/ec-us/v1.0/csprd03/xacml-3.0-ec-us-v1.0-csprd03.pdf

Previous version:

http://docs.oasis-open.org/xacml/3.0/ec-us/v1.0/csprd02/xacml-3.0-ec-us-v1.0-csprd02.doc (Authoritative)
http://docs.oasis-open.org/xacml/3.0/ec-us/v1.0/csprd02/xacml-3.0-ec-us-v1.0-csprd02.html
http://docs.oasis-open.org/xacml/3.0/ec-us/v1.0/csprd02/xacml-3.0-ec-us-v1.0-csprd02.pdf

Latest version:

http://docs.oasis-open.org/xacml/3.0/ec-us/v1.0/xacml-3.0-ec-us-v1.0.doc (Authoritative)
http://docs.oasis-open.org/xacml/3.0/ec-us/v1.0/xacml-3.0-ec-us-v1.0.html
http://docs.oasis-open.org/xacml/3.0/ec-us/v1.0/xacml-3.0-ec-us-v1.0.pdf

Technical Committee:

OASIS eXtensible Access Control Markup Language (XACML) TC

Chairs:

Bill Parducci (bill@parducci.net), Individual member
Hal Lockhart (hal.lockhart@oracle.com), Oracle

Editors:

John Tolbert (john.w.tolbert@boeing.com), The Boeing Company
Paul Tyson (ptyson@bellhelicopter.textron.com), Bell Helicopter Textron
Richard C. Hill (richard.c.hill@boeing.com), The Boeing Company

Related work:

This specification is related to:

- *eXtensible Access Control Markup Language (XACML) Version 3.0.* 22 January 2013. OASIS Standard. http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html.

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 OASIS eXtensible Access Control Markup Language (XACML) TC on the above date. The level of approval is also listed above. Check the "Latest version" location noted above for possible later revisions of this document.

Copyright © OASIS Open 2013. All Rights Reserved.

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).

Citation format:

When referencing this specification the following citation format should be used:

[xacml-ec-us-v1.0]

XACML 3.0 Export Compliance US (EC-US) Profile Version 1.0. 10 January 2013. OASIS Committee Specification Draft 05 / Public Review Draft 03. http://docs.oasis-open.org/xacml/3.0/ec-us/v1.0/csprd03/xacml-3.0-ec-us-v1.0-csprd03.html.

Copyright © OASIS Open 2013. All Rights Reserved.

Notices

Copyright © OASIS Open 2013. 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 name "OASIS" is a trademark 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/policies-guidelines/trademark 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 7
1.6 Disclaimer 7
2 Profile 8
2.1 Resource Attributes 8
2.1.1 Jurisdiction 8
2.1.2 ECCN 8
2.1.3 USML 8
2.1.4 Authority-to-export 8
2.1.5 Effective-Date 9
2.1.6 Expiration-Date 9
2.1.7 Work-effort 9
2.2 Subject Attributes 9
2.2.1 Nationality 9
2.2.2 Current nationality 9
2.2.3 Location 9
2.2.4 Organization 10
2.2.5 US Person 10
3 Identifiers 11
3.1 Profile Identifier 11
4 Examples (non-normative) 12
4.1 Commerce Control List rule 12
4.2 State Department agreement 13
5 Conformance 16
5.1 Attribute Identifiers 16
5.2 Attribute Values 16
Appendix A. Acknowledgements 18
Appendix B. Revision History 21

Copyright © OASIS Open 2013. All Rights Reserved.

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

Authority-to-export

A legal agreement authorizing exports. An export license is an example of an authorization document between the authoritative agency and an organization which has requested an exception to allow exports to otherwise prohibited locations. "NLR" (No License Required) indicates that no export license is required for the export of the item in question.

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***.

Effective date

The date on which an authorization document or export license takes effect, thereby implying access for authorized purposes.

Expiration date

Copyright © OASIS Open 2013. All Rights Reserved.

The date on which an authorization document or export license expires, thereby terminating access.

ITAR

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

Jurisdiction

The US department which governs the applicable export regulations: either Department of Commerce for EAR or Department of State for ITAR.

Location

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

Nationality

A country of which a person is a citizen.

Organization

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

USML

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

US Person

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

Work effort

This attribute can be used to indicate the specific work effort, statement of work, project, or program which is associated with the export-controlled resource. This attribute provides additional granularity to limit access to users within organizations to those with a specific need to know for a given work effort.

1.2 Terminology

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

1.3 Normative References

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

[XACML] OASIS, Committee Draft 02, 21 January 2010, *eXtensible Access Control Markup Language (XACML) Version 3.0,* http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-cd-04-en.doc.

1.4 Non-Normative References

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

[DDTC] US Department of State Directorate of Defense Trade Controls, http://www.pmddtc.state.gov/.

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

Copyright © OASIS Open 2013. All Rights Reserved.

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

1.5 Scope

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

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

1.6 Disclaimer

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

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

Copyright © OASIS Open 2013. All Rights Reserved.

2 Profile

2.1 Resource Attributes

2.1.1 Jurisdiction

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

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

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

2.1.2 ECCN

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

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

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

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

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

```
9A120
```

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

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

- Items without an ECCN may be identified as “EAR99”.
- All comparisons shall be case-sensitive.

2.1.3 USML

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

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

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

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

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

```
VIII(i)
```

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

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

- All comparisons shall be case-sensitive.

2.1.4 Authority-to-export

Authorization-document values shall be designated with the following attribute identifier:

```
urn:oasis:names:tc:xacml:3.0:ec-us:resource:authority-to-export
```

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

Copyright © OASIS Open 2013. All Rights Reserved.

Authority-to-export values may include “EAR99”, “NLR” (No License Required), or the type of license as well as license numbers for tracking. Examples of license types include TAA (Technical Assistance Agreement, a type of ITAR license), MLA (Manufacturing License Agreement, a type of ITAR license), or EAR. Examples of attribute values could be TA1234-56 or AG1234-56.

2.1.5 Effective-Date

Effective-date values shall be designated with the following attribute identifier:

```
urn:oasis:names:tc:xacml:3.0:ec-us:resource:effective-date
```

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

This attribute can be used to indicate the date on which an export license takes effect, thereby implying access for authorized purposes.

2.1.6 Expiration-Date

Expiration-date values shall be designated with the following attribute identifier:

```
urn:oasis:names:tc:xacml:3.0:ec-us:resource:expiration-date
```

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

The date on which an export license expires, thereby terminating access.

2.1.7 Work-effort

Work-effort values shall be designated with the following attribute identifier:

```
urn:oasis:names:tc:xacml:3.0:ec-us:resource:work-effort
```

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

This attribute can be used to indicate the specific work effort, statement of work, project, or program which is associated with the export-controlled resource. This attribute provides additional granularity to limit access to users within organizations to those with a specific need to know for a given work effort.

2.2 Subject Attributes

2.2.1 Nationality

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

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

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

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

2.2.2 Current nationality

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

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

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

2.2.3 Location

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

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


Copyright © OASIS Open 2013. All Rights Reserved.

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

185 2.2.4 Organization

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

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

189 The DataType of this attribute is http://www.w3.org/2001/XMLSchema#string.

190

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

193 2.2.5 US Person

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

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

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

Copyright © OASIS Open 2013. All Rights Reserved.

3 Identifiers

This profile defines the following URN identifiers.

3.1 Profile Identifier

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

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


Copyright © OASIS Open 2013. All Rights Reserved.

4 Examples (non-normative)

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

The following entity definitions are used in these examples

```
<!ENTITY ec-us-subj "urn:oasis:names:tc:xacml:3.0:ec-us:subject:">
<!ENTITY ec-us-res "urn:oasis:names:tc:xacml:3.0:ec-us:resource:">
<!ENTITY func10 "urn:oasis:names:tc:xacml:1.0:function:">
<!ENTITY resource_category
   "urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
<!ENTITY subject_category
   "urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
<!ENTITY xacml-res "urn:oasis:names:tc:xacml:1.0:resource:">
<!ENTITY xs "http://www.w3.org/2001/XMLSchema#">
<!ENTITY rca "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:">
```

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

4.1 Commerce Control List rule

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

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

```
[a1]   <Policy
[a2]     xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
[a3]     PolicyId="urn:oasis:names:tc:xacml:3.0:ec-us:example:CCL"
[a4]     RuleCombiningAlgId="&rca;first-applicable"
[a5]     Version="1.0">
[a6]     <Description>Simple rule for one ECCN.</Description>
[a7]     <Target/>
[a8]     <VariableDefinition VariableId="AT1">
[a9]       <Apply FunctionId="&func10;any-of-any">
[a10]        <Function FunctionId="&func10;string-equal"/>
[a11]        <Apply FunctionId="&func10;string-union">
[a12]          <AttributeDesignator
[a13]            AttributeId="&ec-us-subj;current-nationality"
[a14]            Category="&subject_category;"
[a15]            DataType="&xs;string"
[a16]            MustBePresent="false"/>
[a17]          <AttributeDesignator
[a18]            AttributeId="&ec-us-subj;location"
[a19]            Category="&subject_category;"
[a20]            DataType="&xs;string"
[a21]            MustBePresent="false"/>
[a22]        </Apply>
[a23]        <Apply FunctionId="&func10;string-bag">
[a24]          <AttributeValue DataType="&xs;string">SD</AttributeValue>
[a25]          <AttributeValue DataType="&xs;string">SY</AttributeValue>
[a26]        </Apply>
[a27]      </Apply>
[a28]    </VariableDefinition>
[a29]    <VariableDefinition VariableId="NP1">
[a30]      <Apply FunctionId="&func10;any-of-any">
[a31]        <Function FunctionId="&func10;string-equal"/>
[a32]        <Apply FunctionId="&func10;string-union">
[a33]          <AttributeDesignator
[a34]            AttributeId="&ec-us-subj;current-nationality"
[a35]            Category="&subject_category;"
[a36]            DataType="&xs;string"
[a37]            MustBePresent="false"/>
```


Copyright © OASIS Open 2013. All Rights Reserved.

```
[a38]          <AttributeDesignator
[a39]            AttributeId="&ec-us-subj;location"
[a40]            Category="&subject_category;"
[a41]            DataType="&xs;string"
[a42]            MustBePresent="false"/>
[a43]        </Apply>
[a44]        <Apply FunctionId="&func10;string-bag">
[a45]          <AttributeValue DataType="&xs;string">IR</AttributeValue>
[a46]          <AttributeValue DataType="&xs;string">PK</AttributeValue>
[a47]        </Apply>
[a48]      </Apply>
[a49]    </VariableDefinition>
[a50]    <Rule Effect="Deny" RuleId="3A980">
[a51]      <Description>
[a52]          Voice print identification and analysis equipment and parts"
[a53]      </Description>
[a54]      <Target>
[a55]        <AnyOf>
[a56]          <AllOf>
[a57]            <Match MatchId="&func10;string-regexp-match">
[a58]              <AttributeValue DataType="&xs;string">^3A980.*</AttributeValue>
[a59]              <AttributeDesignator
[a60]                AttributeId="&ec-us-res;eccn"
[a61]                Category="&resource_category;"
[a62]                DataType="&xs;string"
[a63]                MustBePresent="false"/>
[a64]            </Match>
[a65]          </AllOf>
[a66]        </AnyOf>
[a67]      </Target>
[a68]      <Condition>
[a69]        <Apply FunctionId="&func10;or">
[a70]          <VariableReference VariableId="AT1"/>
[a71]          <VariableReference VariableId="NP1"/>
[a72]        </Apply>
[a73]      </Condition>
[a74]    </Rule>
[a75]  </Policy>
```

[a8-a28] Define a variable that returns true if the subject's `current-nationality` or `location` is "SD" or "SY". These are the countries listed under the anti-terrorism reason for control in the ***CCL***.

[a29-a49] Define another variable to check if `current-nationality` or `location` is in the group of countries controlled for nuclear non-proliferation.

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

[a50] Define a rule that applies to resources with an ***ECCN*** classification (`eccn`) of "3A980".

[a68-a73] Test if subject has a `current-nationality` or `location` that is controlled for this classification.

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

4.2 State Department agreement

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

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

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

Copyright © OASIS Open 2013. All Rights Reserved.

```
[b1]      <Policy
[b2]        xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
[b3]        PolicyId="TA-XYZ-00"
[b4]        RuleCombiningAlgId="&rca;first-applicable"
[b5]        Version="1.0">
[b6]        <Description>
[b7]          Permit exports to Canadian and Brazilian partners.
[b8]        </Description>
[b9]        <Target>
[b10]         <AnyOf>
[b11]           <AllOf>
[b12]             <Match MatchId="&func10;string-regexp-match">
[b13]               <AttributeValue DataType="&xs;string">EXP$</AttributeValue>
[b14]               <AttributeDesignator
[b15]                 AttributeId="&xacml-res;resource-id"
[b16]                 Category="&resource_category;"
[b17]                 DataType="&xs;string"
[b18]                 MustBePresent="false"/>
[b19]             </Match>
[b20]             <Match MatchId="&func10;string-equal">
[b21]               <AttributeValue DataType="&xs;string">ITAR</AttributeValue>
[b22]               <AttributeDesignator
[b23]                 AttributeId="&ec-us-res;jurisdiction"
[b24]                 Category="&resource_category;"
[b25]                 DataType="&xs;string"
[b26]                 MustBePresent="false"/>
[b27]             </Match>
[b28]           </AllOf>
[b29]         </AnyOf>
[b30]         <AnyOf>
[b31]           <AllOf>
[b32]             <Match MatchId="&func10;string-equal">
[b33]               <AttributeValue DataType="&xs;string"
[b34]                 >BrazilEnterprise</AttributeValue>
[b35]               <AttributeDesignator
[b36]                 AttributeId="&ec-us-subj;organization"
[b37]                 Category="&subject_category;"
[b38]                 DataType="&xs;string"
[b39]                 MustBePresent="false"/>
[b40]             </Match>
[b41]           </AllOf>
[b42]           <AllOf>
[b43]             <Match MatchId="&func10;string-equal">
[b44]               <AttributeValue DataType="&xs;string"
[b45]                 >CanadianEnterprise</AttributeValue>
[b46]               <AttributeDesignator
[b47]                 AttributeId="&ec-us-subj;organization"
[b48]                 Category="&subject_category;"
[b49]                 DataType="&xs;string"
[b50]                 MustBePresent="false"/>
[b51]             </Match>
[b52]           </AllOf>
[b53]         </AnyOf>
[b54]       </Target>
[b55]       <VariableDefinition VariableId="TA-XYZ-00-nationalities">
[b56]         <Apply FunctionId="&func10;string-subset">
[b57]           <AttributeDesignator
[b58]             AttributeId="&ec-us-subj;nationality"
[b59]             Category="&subject_category;"
[b60]             DataType="&xs;string"
[b61]             MustBePresent="false"/>
[b62]           <Apply FunctionId="&func10;string-bag">
[b63]             <AttributeValue DataType="&xs;string">BR</AttributeValue>
[b64]             <AttributeValue DataType="&xs;string">CA</AttributeValue>
```

 Copyright © OASIS Open 2013. All Rights Reserved.

```
[b65]           </Apply>
[b66]         </Apply>
[b67]       </VariableDefinition>
[b68]       <Rule Effect="Permit" RuleId="permit-TA-XYZ-00">
[b69]         <Target>
[b70]           <AnyOf>
[b71]             <AllOf>
[b72]               <Match MatchId="&func10;string-equal">
[b73]                 <AttributeValue DataType="&xs;string"
[b74]                   >VIII(h)</AttributeValue>
[b75]                 <AttributeDesignator
[b76]                   AttributeId="&ec-us-res;usml"
[b77]                   Category="&resource_category;"
[b78]                   DataType="&xs;string"
[b79]                   MustBePresent="false"/>
[b80]               </Match>
[b81]             </AllOf>
[b82]           </AnyOf>
[b83]         </Target>
[b84]         <Condition>
[b85]           <VariableReference VariableId="TA-XYZ-00-nationalities"/>
[b86]         </Condition>
[b87]       </Rule>
[b88]     </Policy>
```

[b10-b29] This policy applies to resources with `resource-id` ending in “EXP” that have `jurisdiction` equal to “ITAR”.

[b30-b53] This policy applies to subjects who work for (have `organization` attribute) of “BrazilianEnterprise” or “CanadianEnterprise”.

[b55-b67] Define a variable to test that all `nationality` values are in the set (“BR”, “CA”).

[b68-b87] Define a rule that permits access if the `usml` is “VIII(h)” and the subject’s `nationality` values are all in the specified set.

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

Copyright © OASIS Open 2013. All Rights Reserved.

5 Conformance

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

5.1 Attribute Identifiers

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

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

Identifiers	
urn:oasis:names:tc:xacml:3.0:ec-us:resource:jurisdiction	M
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:resource:authority-to-export	M
urn:oasis:names:tc:xacml:3.0:ec-us:resource:effective-date	M
urn:oasis:names:tc:xacml:3.0:ec-us:resource:expiration-date	M
urn:oasis:names:tc:xacml:3.0:ec-us:resource:work-effort	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:organization	M
urn:oasis:names:tc:xacml:3.0:ec-us:subject:us-person	M
urn:oasis:names:tc:xacml:3.0:ec-us:subject:location	M

5.2 Attribute Values

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

Copyright © OASIS Open 2013. All Rights Reserved.

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

 Copyright © OASIS Open 2013. All Rights Reserved.

Appendix A. Acknowledgements

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

Participants:

John Tolbert, The Boeing Company
Paul Tyson, Bell Helicopter Textron
Richard Hill, The Boeing Company

Committee members during profile development:

Person	Organization	Role
David Brossard	Axiomatics	Voting Member
Gerry Gebel	Axiomatics	Member
Srijith Nair	Axiomatics	Member
Erik Rissanen	Axiomatics	Voting Member
Richard Skedd	BAE SYSTEMS plc	Member
Abbie Barbir	Bank of America	Member
Radu Marian	Bank of America	Member
Rakesh Radhakrishnan	Bank of America	Member
Paul Tyson	Bell Helicopter Textron Inc.	Voting Member
Ronald Jacobson	CA Technologies	Member
Masum Hasan	Cisco Systems	Member
Anil Tappetla	Cisco Systems	Member
Gareth Richards	EMC	Member
Remon Sinnema	EMC	Voting Member
Matt Crooke	First Point Global Pty Ltd.	Member
Allan Foster	Forgerock Inc.	Member
Michiharu Kudo	IBM	Member
Sridhar Muppidi	IBM	Member
Vernon Murdoch	IBM	Member

Copyright © OASIS Open 2013. All Rights Reserved.

Nataraj Nagaratnam	IBM	Member
Gregory Neven	IBM	Member
Franz-Stefan Preiss	IBM	Member
Ron Williams	IBM	Member
David Chadwick	Individual	Member
David Choy	Individual	Member
Bill Parducci	Individual	Chair
Richard Sand	Individual	Member
Mike Schmidt	Individual	Member
David Staggs	Jericho Systems	Voting Member
Thomas Hardjono	M.I.T.	Member
Anthony Nadalin	Microsoft	Voting Member
Andy Han	NextLabs, Inc.	Member
Naomaru Itoi	NextLabs, Inc.	Member
Kamalendu Biswas	Oracle	Member
Willem de Pater	Oracle	Member
Subbu Devulapalli	Oracle	Member
Rich Levinson	Oracle	Secretary
Hal Lockhart	Oracle	Chair
Sid Mishra	Oracle	Member
Prateek Mishra	Oracle	Member
Roger Wigenstam	Oracle	Member
YanJiong WANG	Primeton Technologies, Inc.	Member
Danny Thorpe	Quest Software	Voting Member
Kenneth Peeples	Red Hat	Member
Anil Saldhana	Red Hat	Member
Darran Rolls	SailPoint Technologies	Member

Copyright © OASIS Open 2013. All Rights Reserved.

Jan Herrmann	Siemens AG	Member
Crystal Hayes	The Boeing Company	Voting Member
Richard Hill	The Boeing Company	Voting Member
John Tolbert	The Boeing Company	Voting Member
Jean-Paul Buu-Sao	Transglobal Secure Collaboration Participation, Inc. (TSCP)	Voting Member
Martin Smith	US Department of Homeland Security	Member
John Davis	Veterans Health Administration	Voting Member
Duane DeCouteau	Veterans Health Administration	Member
Mohammad Jafari	Veterans Health Administration	Voting Member
Steven Legg	ViewDS	Voting Member
Johann Nallathamby	WSO2	Member
Asela Pathberiya	WSO2	Member
Prabath Siriwardena	WSO2	Member

Copyright © OASIS Open 2013. All Rights Reserved.

Appendix B. Revision History

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
CD3	2/11/2010	Paul Tyson	Updated table of contents
WD3	11/28/2012	John Tolbert	Changed “Classification” to “Jurisdiction”, added “License” as a resource attribute, and updated membership list.
WD4	6/4/2012	John Tolbert/Paul Tyson/Richard Hill	Changed “License” to “Authorization-document”, and added “Effective-date” and “Expiration-date”. Added DataType to ECCN, USML, and Organization attributes. Updated examples.
CSD5	12/13/2012	John Tolbert/Richard hill	Changed “Authorization-document” to “Authority-to-export”, added “Work-effort” as resource attribute.

Copyright © OASIS Open 2013. All Rights Reserved.