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)

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

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

The non-normative errata page for this specification is located at http://www.oasis-open.org/committees/xacml/.
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 ....................................................................................................................... 15

C. Revision History................................................................................................................................. 15

Error! Bookmark not defined.
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
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.

### 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


### 1.4 Non-Normative References


### 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.
2 Profile

2.1 Resource Attributes

2.1.1 Classification

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:classification

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

2.1.1 ECCN

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

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

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

2.1.2 USML

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

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

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.
- Additional balanced parentheses may be appended to the minimal value (or pattern), corresponding to subparagraph designations in the USML.
- All comparisons shall be case-sensitive.

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
```

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].

### 2.2.4 Organization

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

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

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

### 2.2.5 US Person

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

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

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

```xml
<!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#"/>
```

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”**.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<Policy xmlns="urn:oasis:names:tc:xacml:3.0:schema:os"
    PolicyId="urn:oasis:names:tc:xacml:3.0:ec-us:example:CCL"
    Version="1.0"
    RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable">
    <Description>
        Simple rule for one ECCN.
    </Description>
    <Target/>
    <VariableDefinition VariableId="AT1">
        <!-- Anti-terrorism -->
        <Apply FunctionId="&func10;any-of-any"/>
        <Function FunctionId="&func10;string-equal"/>
        <Apply FunctionId="&func10;string-union"/>
        <AttributeDesignator
            Category="&subject_category;"
            AttributeId="&ec-us-subj;current-nationality"/>
        <AttributeDesignator
            Category="&subject_category;"
            AttributeId="&ec-us-subj;location"/>
    </VariableDefinition>
    <VariableDefinition VariableId="NP1">
        <!-- similar to AT1 -->
        <Apply FunctionId="&func10;any-of-any"/>
        <Function FunctionId="&func10;string-equal"/>
        <Apply FunctionId="&func10;string-union"/>
        <AttributeDesignator
            Category="&subject_category;"
            AttributeId="&ec-us-subj;current-nationality"/>
        <AttributeDesignator
            Category="&subject_category;"
            AttributeId="&ec-us-subj;location"/>
    </VariableDefinition>
    <Rule RuleId="3A980" Effect="Deny">
        <Description>
            Voice print identification and analysis equipment and parts...
        </Description>
        <Target/>
    </Rule>
</Policy>
```
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.

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.

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

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".

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.

Define a rule that applies to resources with an ECCN classification (eccn) of "3A980".

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]).
[b20]  <!-- Subject must work for a partner organization -->
[b21]  <AllOf>
[b22]    <Match MatchId="&func10;string-equal">
[b23]      <AttributeValue DataType="&xs;string">
[b24]        BrazilEnterprise
[b25]      </AttributeValue>
[b26]      <AttributeDesignator Category="&subject_category;"
[b27]          AttributeId="&ec-us-subj;organization" />
[b28]    </Match>
[b29]  </AllOf>
[b30]  <AllOf>
[b31]    <Match MatchId="&func10;string-equal">
[b32]      <AttributeValue DataType="&xs;string">
[b33]        CanadianEnterprise
[b34]      </AttributeValue>
[b35]      <AttributeDesignator Category="&subject_category;"
[b36]          AttributeId="&ec-us-subj;organization"/>
[b37]    </Match>
[b38]  </AllOf>
[b39]  </AnyOf>
[b40]  </Target>
[b41]  <VariableDefinition VariableId="TA-XYZ-00-nationalities">
[b42]    <!-- Subject must hold no nationalities other than “BR”, “CA” -->
[b43]    <Apply FunctionId="&func10;string-subset">
[b44]      <AttributeDesignator MustBePresent="false"
[b45]          Category="&subject_category;"
[b46]          AttributeId="&ec-us-subj;nationality"
[b47]          DataType="&xs;string"/>
[b48]      <Apply FunctionId="&func10;string-bag">
[b49]        <AttributeValue DataType="&xs;string">BR</AttributeValue>
[b50]        <AttributeValue DataType="&xs;string">CA</AttributeValue>
[b51]      </Apply>
[b52]    </Apply>
[b53]  </VariableDefinition>
[b54]  <Rule RuleId="permit-TA-XYZ-00" Effect="Permit">
[b55]    <Target>
[b56]      <AnyOf>
[b57]        <AllOf>
[b58]          <Match MatchId="&func10;string-equal">
[b59]            <AttributeValue
[b60]              Category="&resource_category;"
[b61]              DataType="&xs;string">VIII(h)</AttributeValue>
[b62]            <AttributeDesignator Category="&resource_category;"
[b63]              AttributeId="&ec-us-res;usml"/>
[b64]          </Match>
[b65]        </AllOf>
[b66]      </AnyOf>
[b67]    </Target>
[b68]    <Condition>
[b69]      <VariableReference VariableId="TA-XYZ-00-nationalities"/>
[b70]    </Condition>
[b71]  </Rule>
[b72] </Policy>

[b5-b18] This policy applies to resources with resource-id ending in “EXP” that have classification equal to “ITAR”.
[b19-b39] This policy applies to subjects who work for (have organization attribute) of “BrazilianEnterprise” or “CanadianEnterprise”.
[b41-b54] Define a variable to test that all nationality values are in the set (“BR”, “CA”).
[b55-b71] 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.
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.

<table>
<thead>
<tr>
<th>Identifiers</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>urn:oasis:names:tc:xacml:3.0:ec-us:resource:eccn</td>
<td>M</td>
</tr>
<tr>
<td>urn:oasis:names:tc:xacml:3.0:ec-us:resource:usml</td>
<td>M</td>
</tr>
<tr>
<td>urn:oasis:names:tc:xacml:3.0:ec-us:subject:nationality</td>
<td>M</td>
</tr>
<tr>
<td>urn:oasis:names:tc:xacml:3.0:ec-us:subject:current-nationality</td>
<td>M</td>
</tr>
<tr>
<td>urn:oasis:names:tc:xacml:3.0:ec-us:subject:location</td>
<td>M</td>
</tr>
<tr>
<td>urn:oasis:names:tc:xacml:3.0:ec-us:subject:organization</td>
<td>M</td>
</tr>
<tr>
<td>urn:oasis:names:tc:xacml:3.0:ec-us:subject:us-person</td>
<td>M</td>
</tr>
</tbody>
</table>

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).

NOTE: In order to process conformant XACML policies and requests correctly, PIP and PEP modules may have to translate native data values into the datatypes and formats specified in this profile.
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, Associate
### B. Revision History

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