CARML Profile of the Liberty Privacy Constraints Specification

Version 1.0

Editors:
Phil Hunt, Oracle Corporation

Contributors:
Prateek Mishra, Oracle Corporation

Abstract:
This profile profiles the use of privacy constraints within CARML. It defines roles and URIs used when privacy constraints are used to constrain CARML interactions, roles, predicates or attributes.

Filename: liberty-igf-carml-profile-privcon-v1.0.pdf
NOTICE:
This document has been prepared by Sponsors of the Liberty Alliance. Permission is hereby granted to use the document solely for the purpose of implementing the Specification. No rights are granted to prepare derivative works of this Specification. Entities seeking permission to reproduce portions of this document for other uses must contact the Liberty Alliance to determine whether an appropriate license for such use is available.

Implementation or use of certain elements of this document may require licenses under third party intellectual property rights, including without limitation, patent rights. The Sponsors of and any other contributors to the Specification are not and shall not be held responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights. This Specification is provided "AS IS," and no participant in the Liberty Alliance makes any warranty of any kind, express or implied, including any implied warranties of merchantability, non-infringement of third party intellectual property rights, and fitness for a particular purpose. Implementers of this Specification are advised to review the Liberty Alliance Project's website (http://www.projectliberty.org/) for information concerning any Necessary Claims Disclosure Notices that have been received by the Liberty Alliance Management Board.

Copyright © 2007-2009
CARML Profile of the Liberty Privacy Constraints Specification
94 Contents

95 1 Introduction 5
96 1.1 Example 5
97 1.2 Terminology 6
98 1.3 References 6
99 1.3.1 Normative References 6
100 1.3.2 Non-Normative References 7
101 1.4 Notation 7

102 2 Profile 8
103 2.1 Issuer Attribute 8
104 2.2 PurposeConstraint 8
105 2.3 PropagateConstraint 8
106 2.3.1 Example 9
107

108
1 Introduction

Privacy constraints are utilized in CARML documents, describing constraints on the use of identity data by services or applications.

These constraints may be contributed by:

- developers – reflecting decisions and implementation choices made during design and implementation. For example, whether identity data is persisted and, if so, whether it is encrypted.

- deployers – reflecting practice and choices made during service deployment. For example, the purpose for which identity is being sought or whether identity data would be propagated further to certain endpoints.

This document builds on the Liberty Privacy Constraints [PrivCon] specification by defining additional URIs needed to specify constraints for CARML elements. Developers and deployers would use WS-Policy [WS-Policy] constructs to create composite constraints based on the unitary privacy constraints given in [PrivCon].

1.1 Example

The following is an example of a privacy constraint used with CARML.

```xml
<wsp:Policy>
  <wsp:All>
    <pri:PurposeConstraint
      Entity="urn:lap:names:1.0:igf:pri:entity:deployer">
      ref="urn:mycorp:2007:marketing"/>
    <pri:PropagateConstraint
      Entity="urn:lap:names:1.0:igf:pri:entity:developer">
      ref="urn:lap:names:1.0:igf:pri:propagate:requestor"/>
    <pri:RetentionConstraint
      Entity="urn:lap:names:1.0:igf:pri:entity:developer">
      ref="urn:lap:names:1.0:igf:pri:retention:transient">
      <pri:LifetimeConstraint>
        <pri:Minutes>59</pri:Minutes>
        <pri:Hours>23</pri:Hours>
      </pri:LifetimeConstraint>
    </pri:RetentionConstraint>
  </wsp:All>
</wsp:Policy>
```
Lines [a1]-[a2] and [a17]-[a18] illustrate the use of WS-Policy to aggregate multiple atomic privacy constraints into a single policy object. Such a policy object might be published by an application or service in combination with a request for identity data. [a3]-[a5] indicate the purpose for which data is sought. [a6]-[a8] indicate that the data items will not be propagated outside the administrative domain within which the service operates. [a9]-[a16] indicate that data items will not be persisted to store, and that they will only be cached in memory for a maximum period of 23 hours and 59 minutes.

1.2 Terminology

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

<table>
<thead>
<tr>
<th>Prefix</th>
<th>XML Namespace</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>pri:</td>
<td>urn:liberty:names:1.0:igf:pri</td>
<td>Namespace defined in Privacy Constraints Specification</td>
</tr>
<tr>
<td>wsp:</td>
<td><a href="http://www.w3.org/ns/ws-policy">http://www.w3.org/ns/ws-policy</a></td>
<td>Web Services Policy namespace</td>
</tr>
<tr>
<td>xs:</td>
<td><a href="http://www.w3.org/2001/XMLSchema">http://www.w3.org/2001/XMLSchema</a></td>
<td>This namespace is defined in the W3C XML Schema specification [XML-Schema1]. In schema listings, this is the default namespace and no prefix is shown. For clarity, the prefix is generally shown in specification text when XML Schema-related constructs are mentioned.</td>
</tr>
<tr>
<td>xsi:</td>
<td><a href="http://www.w3.org/2001/XMLSchema-instance">http://www.w3.org/2001/XMLSchema-instance</a></td>
<td>This namespace is defined in the W3C XML Schema specification [XML-Schema1] for schema-related markup that appears in XML instances.</td>
</tr>
</tbody>
</table>

1.3 References

1.3.1 Normative References


1.3.2 Non-Normative References

None

1.4 Notation

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

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

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

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

2.1 Issuer Attribute

<table>
<thead>
<tr>
<th>URI</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>urn:lap:names:1.0:igf:pri:entity:developer</td>
<td>Indicates that the assertion was contributed by the developer</td>
</tr>
<tr>
<td>urn:lap:names:1.0:igf:pri:entity:deployed</td>
<td>Indicates that the assertion was contributed by the deployer</td>
</tr>
</tbody>
</table>

2.2 PurposeConstraint

Multiple instances of the <priv:PurposeConstraint> element MAY be contributed by both developers and deployers.

2.3 PropagateConstraint

Multiple instances of the <priv:PropagateConstraint> element MAY be contributed by both developers and deployers.

An additional attribute EndPointType is defined by this profile:

```
<attribute name="EndPointType" type="anyURI"/>
```

Two URIs are defined for use with this attribute:

<table>
<thead>
<tr>
<th>URI</th>
</tr>
</thead>
<tbody>
<tr>
<td>urn:lap:names:1.0:igf:pri:propagate:service:definition</td>
</tr>
<tr>
<td>urn:lap:names:1.0:igf:pri:propagate:service:endpoint</td>
</tr>
</tbody>
</table>
Developers SHOULD use urn:lap:names:1.0:igf:pri:propagate:service:definition to indicate that they are describing an API or software component to which identity data will be propagated.

Deployers SHOULD use urn:lap:names:1.0:igf:pri:propagate:service:endpoint to indicate the deployed end-points or servers to which identity data will be propagated.

### 2.3.1 Example

In the first example, a developer indicates that identity data may be propagated to a certain module in a specific software package.

```
<pri:PropagateConstraint
    Entity="urn:lap:names:1.0:igf:pri:entity:developer"
    EndPointType="urn:lap:names:1.0:igf:pri:propagate:service:definition"
    ref="urn:hr-example-product:validation-module"/>
```

In the second example, a deployer indicates that identity data may be propagated to a specific URL.

```
<pri:PropagateConstraint
    Entity="urn:lap:names:1.0:igf:pri:entity:developer"
    EndPointType="urn:lap:names:1.0:igf:pri:propagate:service:endpoint"
    ref="http://www.example.com/partner_relations"/>
```