# CARML Profile of the Liberty IGF Privacy Constraints Specification

Draft Version 1.0-02

**Editors:**

Phil Hunt, Oracle Corporation

**Contributors:**

Prateek Mishra, Oracle Corporation
Eric Tiffany, Liberty Alliance

**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.

# Notice



Liberty Alliance Project
Licensing Administrator
c/o IEEE-ISTO
445 Hoes Lane
Piscataway, NJ 08855-1331, USA
info@projectliberty.org

# Contents

# 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:

1. 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.
2. 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 [PrivConstr] 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 [PrivConstr].

## 1.1. Example

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

```
[a1]  <wsp:Policy>
[a2]  <wsp:All>
[a3]    <pri:PurposeConstraint
[a4]             Entity="urn:lap:names:1.0:igf:pri:entity:deployer">
[a5]             ref="urn:mycorp:2007:marketing"/>
[a6]    <pri:PropagateConstraint
[a7]       Entity="urn:lap:names:1.0:igf:pri:entity:developer">
[a8]       ref="urn:lap:names:1.0:igf:pri:propagate:requestor"/>
[a9]    <pri:RetentionConstraint
[a10]      Entity="urn:lap:names:1.0:igf:pri:entity:developer">
[a11]      ref="urn:lap:names:1.0:igf:pri:retention:transient"
[a12]        <pri:LifetimeConstraint>
[a13]             <pri:Minutes>59</pri:Minutes>
[a14]             <pri:Hours>23</pri:Hours>
[a15]        </pri:LifetimeConstraint>
[a16]    </pri:RetentionConstraint>
[a17]   <wsp:All>
[a18]  </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:

| Prefix | XML Namespace | Comments |
|---|---|---|
| pri: | urn:liberty:names:1.0:igf:pri | Namespace defined in Privacy Constraints Specification |
| wsp: | http://www.w3.org/ns/ws-policy | Web Services Policy namespace |
| xs: | http://www.w3.org/2001/XMLSchema | This namespace is defined in the W3C XML Schema specification [Schema1-2]. 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. |
| xsi: | http://www.w3.org/2001/XMLSchema-instance | This namespace is defined in the W3C XML Schema specification [Schema1-2] for schema-related markup that appears in XML instances. |

## 1.3. References

### 1.3.1. Normative References

**[RFC2119]** S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels," RFC 2119, The Internet Engineering Task Force (March 1997). http://www.ietf.org/rfc/rfc2119.txt

**[WS-Policy]** Web Services Polict 1.5 – Framework, October 2007. http://www.w3.org/TR/2004/REC-xmlschema-1-20041028/

**[PrivConstr]** Madsen, Paul, "Liberty IGF Privacy Constraints Specification," Draft Version 1.0-04, Liberty Alliance Project (21 June 2008). http://www.projectliberty.org/specs

**[Schema1-2]** Thompson, Henry S., Beech, David, Maloney, Murray, Mendelsohn, Noah, eds. (28 October 2004). "XML Schema Part 1: Structures Second Edition," Recommendation, World Wide Web Consortium, http://www.w3.org/TR/xmlschema-1/

### 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

| URI | Meaning |
|---|---|
| urn:lap:names:1.0:igf:pri:entity:developer | Indicates that the assertion was contributed by the developer |
| urn:lap:names:1.0:igf:pri:entity:deployer | Indicates that the assertion was contributed by the deployer |

## 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:PurposeConstraint> element MAY be contributed by both developers and deployers.

Developers SHOULD use this constraint to describe an API or software component to which identity data will be propagated.

Deployers SHOULD use this constraint 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.

```
[a19]  <pri:PropagateConstraint
[a20]          Entity="urn:lap:names:1.0:igf:pri:entity:developer"
[a21]          EndPointType="urn:lap:names:1.0:igf:pri:propagate:service:definition"
[a22]          ref="urn:hr-example-product:validation-module"/>
```

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

```
[a23]  <pri:PropagateConstraint
[a24]          Entity="urn:lap:names:1.0:igf:pri:entity:developer"
[a25]          EndPointType="urn:lap:names:1.0:igf:pri:propagate:service:endpoint"
[a26]          ref="http://www.example.com/partner_relations"/>
```