



1 **CARML Profile of the Liberty IGF Privacy** 2 **Constraints Specification**

3 Draft Version 1.0-02

4 **Editors:**

5 Phil Hunt, Oracle Corporation

6 **Contributors:**

7 Prateek Mishra, Oracle Corporation

8 Eric Tiffany, Liberty Alliance

9 **Abstract:**

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

12

Notice

13 This document has been prepared by Sponsors of the Liberty Alliance. Permission is hereby granted to use the
14 document solely for the purpose of implementing the Specification. No rights are granted to prepare derivative
15 works of this Specification. Entities seeking permission to reproduce portions of this document for other uses must
16 contact the Liberty Alliance to determine whether an appropriate license for such use is available.

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

26 Copyright © 2008 AOL LLC; British Telecommunications plc; Computer Associates International, Inc.; Drummond
27 Group, Inc.; Ericsson; France Télécom; Fugen Solutions, Inc.; GSA Office of Governmentwide Policy; Hewlett-
28 Packard Company; Intel Corporation; Luminance Consulting Services; Neustar, Inc.; New Zealand Government
29 State Services Commission; NEC Corporation; NHK (Japan Broadcasting Corporation) Science & Technical
30 Research Laboratories; Nippon Telegraph and Telephone Corporation; Oracle Corporation; Sun Microsystems, Inc.;
31 Symlabs, Inc.; Zenn New Media. All rights reserved.

32 Liberty Alliance Project
33 Licensing Administrator
34 c/o IEEE-ISTO
35 445 Hoes Lane
36 Piscataway, NJ 08855-1331, USA
37 info@projectliberty.org

38 Contents

39	1 Introduction.....	2
40	1.1 Example.....	3
41	1.2 Terminology	
42	3
43	1.3 References.....	4
44	1.3.1 Normative References.....	4
45	1.3.2 Non-Normative References.....	4
46	1.4 Notation.....	4
47	2 Profile.....	4
48	2.1 Issuer Attribute.....	4
49	2.2 PurposeConstraint.....	5
50	2.3 PropagateConstraint.....	5
51	2.3.1 Example.....	5

52 1. Introduction

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

55 These constraints may be contributed by:

- 56 1. developers – reflecting decisions and implementation choices made during design and implementation. For
57 example, whether identity data is persisted and, if so, whether it is encrypted.
- 58 2. deployers – reflecting practice and choices made during service deployment. For example, the purpose for
59 which identity is being sought or whether identity data would be propagated further to certain endpoints.

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

63 1.1. Example

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

```
65 [a1] <wsp:Policy>  
66 [a2] <wsp>All>  
67 [a3] <pri:PurposeConstraint  
68 [a4]     Entity="urn:lap:names:1.0:igf:pri:entity:deployer">  
69 [a5]     ref="urn:mycorp:2007:marketing"/>  
70 [a6] <pri:PropagateConstraint  
71 [a7]     Entity="urn:lap:names:1.0:igf:pri:entity:developer">  
72 [a8]     ref="urn:lap:names:1.0:igf:pri:propagate:requestor"/>  
73 [a9] <pri:RetentionConstraint  
74 [a10]     Entity="urn:lap:names:1.0:igf:pri:entity:developer">  
75 [a11]     ref="urn:lap:names:1.0:igf:pri:retention:transient"  
76 [a12]     <pri:LifetimeConstraint>  
77 [a13]         <pri:Minutes>59</pri:Minutes>  
78 [a14]         <pri:Hours>23</pri:Hours>  
79 [a15]     </pri:LifetimeConstraint>  
80 [a16] </pri:RetentionConstraint>  
81 [a17] <wsp>All>  
82 [a18] </wsp:Policy>
```

83 Lines [a1]-[a2] and [a17]-[a18] illustrate the use of WS-Policy to aggregate multiple atomic privacy constraints into
84 a single policy object. Such a policy object might be published by an application or service in combination with a
85 request for identity data. [a3]-[a5] indicate the purpose for which data is sought. [a6]-[a8] indicate that the data
86 items will not be propagated outside the administrative domain within which the service operates. [a9]-[a16]
87 indicate that data items will not be persisted to store, and that they will only be cached in memory for a maximum
88 period of 23 hours and 59 minutes.

89 1.2. Terminology

90 Conventional XML namespace prefixes are used throughout the listings in this specification to stand for their
91 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.

92 1.3. References

93 1.3.1. Normative References

- 94 [RFC2119] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels," RFC 2119, The
95 Internet Engineering Task Force (March 1997). <http://www.ietf.org/rfc/rfc2119.txt>
- 96 [WS-Policy] Web Services Polict 1.5 – Framework, October 2007. <http://www.w3.org/TR/2004/REC-xmlschema-1-20041028/>
- 98 [PrivConstr] Madsen, Paul, "Liberty IGF Privacy Constraints Specification," Draft Version 1.0-04, Liberty
99 Alliance Project (21 June 2008). <http://www.projectliberty.org/specs>
- 100 [Schema1-2] Thompson, Henry S., Beech, David, Maloney, Murray, Mendelsohn, Noah, eds. (28 October
101 2004). "XML Schema Part 1: Structures Second Edition," Recommendation, World Wide
102 Web Consortium, <http://www.w3.org/TR/xmlschema-1/>

103 1.3.2. Non-Normative References

104 None.

105 1.4. Notation

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

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

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

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

116 2. Profile

117 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

118 2.2. PurposeConstraint

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

121 2.3. PropagateConstraint

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

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

126 Deployers SHOULD use this constraint to indicate the deployed end-points or servers to which identity data will be
127 propagated.

128 2.3.1. Example

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

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

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

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