

1



2

3

CARML Profile of the Liberty Privacy Constraints Specification

5

6 Version 1.0

7

8 **Editors:**

9 Phil Hunt, Oracle Corporation

10

11 **Contributors:**

12 Prateek Mishra, Oracle Corporation

13

14 **Abstract:**

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

18

19 **Filename:** liberty-igf-carml-profile-privcon-v1.0.pdf

CARML Profile of the Liberty Privacy Constraints Specification

20 NOTICE:

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

27
28 Implementation or use of certain elements of this document may require licenses under
29 third party intellectual property rights, including without limitation, patent rights. The
30 Sponsors of and any other contributors to the Specification are not and shall not be held
31 responsible in any manner for identifying or failing to identify any or all such third party
32 intellectual property rights. This Specification is provided "AS IS," and no participant in
33 the Liberty Alliance makes any warranty of any kind, express or implied, including any
34 implied warranties of merchantability, non-infringement of third party intellectual
35 property rights, and fitness for a particular purpose. Implementers of this Specification
36 are advised to review the Liberty Alliance Project's website
37 (<http://www.projectliberty.org/>) for information concerning any Necessary Claims
38 Disclosure Notices that have been received by the Liberty Alliance Management Board.

39 Copyright © 2007-2009

40 ActivIdentity, Trent Adams, Adetti, Adobe Systems, AOL, BEA Systems, Berne,
41 University of Applied Sciences, Gerald Beuchelt, BIPAC, John Bradley, British
42 Telecommunications plc, Hellmuth Broda, Bronnoysund Register Centre, BUPA, CA,
43 Canada Post Corporation, Center for Democracy and Technology, Chief, Information
44 Office Austria, China Internet Network Information Center (CNNIC), ChoicePoint, Citi,
45 City University, Clarity Security, Dan Combs, Computer & Communications Industry
46 Association, Courion Corporation, Danish Biometrics Research Proj. Consortium, Danish
47 National IT and Telecom Agency, Deny All, Deutsche Telekom AG, DGME, Brian
48 Dilley, Diversinet Corp., Drummond Group Inc., East of England Telematics
49 Development Trust Ltd, EIfEL, Electronics and Telecommunications Research Institute
50 (ETRI), Engineering Partnership in Lancashire, Enterprise Java Victoria Inc., Entr'ouvert,
51 Ericsson, Evidian, Fidelity Investments, Financial Services Technology Consortium
52 (FSTC), Finland National Board of Taxes, Fischer International, France Telecom,
53 Fraunhofer-Gesellschaft, Fraunhofer Institute for Integrated Circuits IIS, Fraunhofer
54 Institute for Secure Information Technology (SIT), Fraunhofer Institut for
55 Experimentelles Software Engineering, Fugen Solutions, Fujitsu Services Oy, Fun
56 Communications GmbH, Gemalto, Giesecke & Devrient GMBH, Global Platform, GSA
57 Office of Governmentwide Policy, Healthcare Financial Management Association
58 (HFMA), Health Information and Management Systems Society (HIMSS), Helsinki
59 Institute of Physics, Jeff Hodges, Hongkong Post, Guy Huntington, Imprivata,

CARML Profile of the Liberty Privacy Constraints Specification

60 Information Card Foundation, Institute of Bioorganic Chemistry Poland, Institute of
61 Information Management of the University, Institut Experimentelles Software
62 Engineering (IESE), Intel Corporation, International Institute of Telecommunications,
63 International Security, Trust and Privacy Alliance, Internet2, Interoperability
64 Clearinghouse (ICH), ISOC, Java Wireless Competency Centre (JWCC), Kantega AS,
65 Kuppinger Cole & Partner, Kuratorium OFFIS e.V., Colin Mallett, Rob Marano,
66 McMaster University, MEDNETWorld.com, Methics Oy, Mortgage Bankers Association
67 (MBA), Mydex, National Institute for Urban Search & Rescue Inc NEC Corporation,
68 Network Applications Consortium (NAC), Neustar, Newspaper Association of America,
69 New Zealand Government State Services Commission, NHK (Japan Broadcasting
70 Corporation) Science & Technical Research Laboratories, Nippon Telegraph and
71 Telephone Company, Nokia Corporation, Nortel, NorthID Oy, Norwegian Agency for
72 Public Management and eGovernment, Norwegian Public Roads Administration, Novell,
73 NRI Pacific, Office of the Information Privacy Commissioner of Ontario, Omnibranch,
74 OpenIAM, Oracle USA, Inc., Organisation Internationale pour la Sécurité des
75 Transactions Électroniques (OISTE), Oslo University, Our New Evolution, PAM Forum,
76 Parity Communications, Inc., PayPal, Phase2 Technology, Ping Identity Corporation,
77 Bob Pinheiro, Platinum Solutions, Postsecondary Electronic Standards Council (PESC),
78 Purdue University, RSA Security, Mary Ruddy, SAFE Bio Pharma, SanDisk
79 Corporation, Shidler Center for Law, Andrew Shikiar, Signicat AS, Singapore Institute of
80 Manufacturing Technology, Software & Information Industry Association, Software
81 Innovation ASA, Sprint Nextel Corporation, Studio Notarile Genghini-SNG, Sunderland
82 City Council, SUNET, Sun Microsystems, SwissSign AG, Technische Universitat Berlin,
83 Telefonica S.A., TeleTrusT, TeliaSonera Mobile Networks AB, TERENA, Thales e-
84 Security, The Boeing Company, The Financial Services Roundtable/BITS, The Open
85 Group, The University of Chicago as Operator of Argonne National Laboratory,
86 TRUSTe, tScheme Limited, UNINETT AS, Universidad Politecnica de Madrid,
87 University of Birmingham, University of Kent, University of North Carolina at Charlotte,
88 University of Ottawa (TTBE), U.S. Department of Defense, VeriSign, Vodafone Group
89 Plc, Web Services Competence Center (WSCC), Zenn New Media

90

91

92 All rights reserved

93

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

109 1 Introduction

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

112 These constraints may be contributed by:

113

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

117

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

121

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

126 1.1 Example

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

128

```
129 [a1] <wsp:Policy>  
130 [a2] <wsp:All>  
131 [a3] <pri:PurposeConstraint  
132 [a4] Entity="urn:lap:names:1.0:igf:pri:entity:deployer">  
133 [a5] ref="urn:mycorp:2007:marketing"/>  
134 [a6] <pri:PropagateConstraint  
135 [a7] Entity="urn:lap:names:1.0:igf:pri:entity:developer">  
136 [a8] ref="urn:lap:names:1.0:igf:pri:propagate:requestor"/>  
137 [a9] <pri:RetentionConstraint  
138 [a10] Entity="urn:lap:names:1.0:igf:pri:entity:developer">  
139 [a11] ref="urn:lap:names:1.0:igf:pri:retention:transient"  
140 [a12] <pri:LifetimeConstraint>  
141 [a13] <pri:Minutes>59</pri:Minutes>  
142 [a14] <pri:Hours>23</pri:Hours>  
143 [a15] </pri:LifetimeConstraint>  
144 [a16] </pri:RetentionConstraint>  
145 [a17] <wsp:All>  
146 [a18] </wsp:Policy>
```

147

CARML Profile of the Liberty Privacy Constraints Specification

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

1.2 Terminology

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

159

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 [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.
xsi:	http://www.w3.org/2001/XMLSchema-instance	This namespace is defined in the W3C XML Schema specification [XML-Schema1] for schema-related markup that appears in XML instances.

160

1.3 References**1.3.1 Normative References**

- 163 **[RFC2119]** S. Bradner, *Key words for use in RFCs to Indicate Requirement*
 164 *Levels*, IETF RFC 2119, March 1997.
 165 <http://www.ietf.org/rfc/rfc2119.txt>
- 166
- 167 **[WS-Policy]** Web Services Policy 1.5 – Framework, October 2007.
 168 <http://www.w3.org/TR/2004/REC-xmlschema-1-20041028/>
- 169
- 170 **[PrivCon]** Privacy Constraints Specification, June 2008

171 **1.3.2 Non-Normative References**

172 None

173 **1.4 Notation**

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

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

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

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

186

187 **2 Profile**188 **2.1 Issuer Attribute**

189

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:deployed	Indicates that the assertion was contributed by the deployer

190

191 **2.2 PurposeConstraint**

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

194 **2.3 PropagateConstraint**

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

197 An additional attribute EndPointerType is defined by this profile:

198 `<attribute name="EndPointerType" type="anyURI"/>`

199 Two URIs are defined for use with this attribute:

200

URI
urn:lap:names:1.0:igf:pri:propagate:service:definition
urn:lap:names:1.0:igf:pri:propagate:service:endpoint

201 Developers SHOULD use urn:lap:names:1.0:igf:pri:propagate:service:definition to
202 indicate that they are describing an API or software component to which identity data will
203 be propagated.

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

206 **2.3.1 Example**

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

209

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

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

220

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

227