

1



2

3 Liberty Alliance Privacy Constraints Specification

4 Version 1.0

5 **Editors:**

6 Paul Madsen, NTT

7 **Contributors:**

8 Prateek Mishra, Oracle

9 **Abstract:**

10 Privacy constraints are atomic constraints on the use, display, retention, storage and propagation
11 of identity data. When combined with policy frameworks such as WS-Policy, such assertions can
12 be used to describe composite constraints on identity data.

13 **Filename:** liberty-igf-privacy-constraints-v1.0.pdf

14 **NOTICE:**

15 This document has been prepared by Sponsors of the Liberty Alliance. Permission is hereby
16 granted to use the document solely for the purpose of implementing the Specification. No rights
17 are granted to prepare derivative works of this Specification. Entities seeking permission to
18 reproduce portions of this document for other uses must contact the Liberty Alliance to
19 determine whether an appropriate license for such use is available.
20

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

31 Copyright © 2007-2009

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

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

78 All rights reserved.

79 **Contents**

| | | | |
|----|--------------------------------------|-----------|------------|
| 80 | 1. Introduction | <u>5</u> | Deleted: 1 |
| 81 | 1.1. Example | <u>5</u> | Deleted: 2 |
| 82 | 1.2. Namespaces | <u>6</u> | Deleted: 3 |
| 83 | 1.3. Notation..... | <u>6</u> | Deleted: 3 |
| 84 | 2. Privacy Constraints..... | <u>8</u> | Deleted: 4 |
| 85 | 2.1. Attributes..... | <u>8</u> | Deleted: 4 |
| 86 | 2.2. PurposeConstraint | <u>8</u> | Deleted: 4 |
| 87 | 2.3. PropagateConstraint | <u>8</u> | Deleted: 4 |
| 88 | 2.4. RetentionConstraint..... | <u>9</u> | Deleted: 5 |
| 89 | 2.4.1. LifetimeConstraint | <u>10</u> | Deleted: 5 |
| 90 | 2.5. DataLossOrBreachConstraint..... | <u>10</u> | Deleted: 6 |
| 91 | 2.6. ContractOrLegalConstraint | <u>11</u> | Deleted: 6 |
| 92 | 2.7. DataMaskConstraint | <u>11</u> | Deleted: 6 |
| 93 | 3. References | <u>11</u> | Deleted: 6 |

Formatted: Font: (Default) Times New Roman, Underline, Font color: Blue

94

109 **1. Introduction**

110 Privacy constraints describe fundamental constraints on the propagation, usage, retention,
111 storage and display of identity data. Increasingly, there is concern regarding appropriate use of
112 identity data and Privacy constraints allow the expressions of constraints over the processing of
113 such data.

114 This document describes a small set of atomic privacy constraints. They are not meant to be
115 exhaustive and we fully expect that communities will define additional assertions based on
116 geography, industry and law.

117 Using policy frameworks such as WS-Policy, authorities (custodians of identity data, end-users)
118 and consumers (applications, enterprises) can use Privacy constraints to describe composite
119 constraints on identity data. For authorities, this takes the form of indicating the conditions under
120 which data is being released; for consumers this takes the form of indicating the conditions that
121 will govern their use of data.

122 Privacy constraints describe conditions under which identity data is sought or released. Exactly
123 how Privacy constraints would be used in practice is outside the scope of this work. Depending
124 in business context, they may be added to message flows in protocols or viewed as meta-data
125 associated with identity data.

126 Generally, when a privacy constraint is bound to a request for some attribute, it is interpreted as a
127 'commitment' the requestor is making with respect to its actions should it receive the attribute,
128 when bound to a response carrying an attribute, a constraint is interpreted as an 'obligation'
129 attendant upon the recipient.

130 This document does not define how the binding of privacy statements to messages or metadata
131 would be secured.

132 **1.1. Example**

133 The following is an example of a privacy constraint within WS-Policy. Such a policy might be
134 offered by a user (or a software agent acting on the users behalf) concerning the release of the
135 user's name, address and phone number to an marketing application. It presents a set of
136 conditions about the treatment of identity data which need to be followed by the application.

```
137 1: <wsp:Policy>  
138 2:   <wsp:All>  
139 3:     <pri:PurposeConstraint  
140 4:       Issuer="urn:liberty:names:1.0:igf:pri:entity:user">  
141 5:       ref="urn:mycorp:2007:marketing"/>  
142 6:     <pri:PropagateConstraint
```

```
143 7:         Issuer="urn:liberty:names:1.0:igf:pri:entity:user">
144 8:         ref="urn:liberty:names:1.0:igf:pri:propagate:requestor"/>
145 9:     <pri:RetentionConstraint
146 10:         Issuer="urn:liberty:names:1.0:igf:pri:entity:user">
147 11:         ref="urn:liberty:names:1.0:igf:pri:retention:transient"
148 12:         <pri:LifetimeConstraint>
149 13:             <pri:Minutes>59</pri:Minutes>
150 14:             <pri:Hours>23</pri:Hours>
151 15:         </pri:LifetimeConstraint>
152 16:     </pri:RetentionConstraint>
153 17: <wsp>All>
154 18:</wsp:Policy>
```

155 [a1]-[a2] and [a17]-[a18] illustrate the use of WS-Policy to aggregate multiple atomic privacy
156 constraints into a single policy object.

157 [a3]-[a5] indicate the purpose for which data is released. [a6]-[a8] indicate that the data items
158 should not be propagated outside the administrative domain within which the service operates.
159 [a9]-[a16] indicate that data items will not be persisted to store, and should be cached in memory
160 for a maximum period of 23 hours and 59 minutes.

161 1.2. Namespaces

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

- 165 • The prefix `pri:` stands for the namespace defined in this specification
166 (`urn:liberty:names:1.0:igf:pri`).
- 167 • The prefix `xs:` stands for the W3C XML schema namespace
168 (`http://www.w3.org/2001/XMLSchema`).
- 169 • The prefix `wsp:` stands for the Web Services Policy (`http://www.w3.org/ns/ws-`
170 `policy`).

171 1.3. Notation

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

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

183 2. Privacy Constraints

184 2.1. Attributes

185 We define a single global attribute describing the entity which issued or contributed the
186 assertion.

```
187 <attribute name="Issuer" type="anyURI"/>
```

188 This specification defines one standard URI value for the Issuer attribute. Other URIs can be
189 defined.

- 190 • urn:liberty:names:1.0:igf:pri:entity:user
 - 191 ○ Indicates that the assertion was contributed by the end-user.

192 2.2. PurposeConstraint

193 Describes the usage context in which data is sought or the context in which data is being
194 provided.

```
195 <element name="PurposeConstraint">  
196   <complexType>  
197     <attribute ref="pri:Issuer"/>  
198     <attribute name="uri" type="anyURI" use="required"/>  
199   </complexType>  
200 </element>
```

201 This specification defines a single standard URI for constraining purpose.

- 202 • urn:liberty:names:1.0:igf:pri:purpose:context
 - 203 ○ Indicates that the purpose for which the data value is sought SHOULD be
204 determined from application context.

205 The application context may be determined in many different ways, including for example, by
206 examining the message carrying the constraint.

207 Our expectation is that communities will define additional URIs based on rules for industry
208 verticals and national jurisdictions.

209 2.3. PropagateConstraint

210 Describes constraints on the services or end-points to which the data may be propagated or
211 forwarded.

```
212 <element name="PropagateConstraint">
213   <complexType>
214     <attribute ref="pri:Issuer"/>
215     <attribute name="uri" type="anyURI" use="required"/>
216   </complexType>
217 </element>
```

218 This specification defines a single standard URI for constraining propagation.

- 219 • urn:liberty:names:1.0:igf:pri:propagate:requestor
- 220 ○ Indicates that the data value MUST NOT be propagated beyond the requestor.

221 Other entities for which it might be relevant to constrain propagation might include service,
222 server, department, end-point, etc. The expectation is that such constraints would be defined in
223 other profiles.

224 2.4. RetentionConstraint

225 Indicates whether the data value can be retained by the requestor, in memory or otherwise, and,
226 optionally the time period for which it can be retained.

```
227 <element name="RetentionConstraint">
228   <complexType>
229     <attribute ref="pri:Issuer"/>
230     <attribute name="uri" type="anyURI" use="required"/>
231   </complexType>
232 </element>
```

233 This specification defines five standard URIs for constraining retention.

- 234 • urn:liberty:names:1.0:igf:pri:retention:nocache
- 235 ○ Indicates that the data value MUST NOT be cached or persisted and should be
236 overwritten after a single use.
- 237 • urn:liberty:names:1.0:igf:pri:retention:transient
- 238 ○ Indicates that the data value MAY be held in memory cache but MUST NOT
239 be persisted.
- 240 • urn:liberty:names:1.0:igf:pri:retention:persist

- 241 ○ Indicates that the data value MAY be persisted.
- 242 ● urn:liberty:names:1.0:igf:pri:retention:persist:encrypt
- 243 ○ Indicates that the data value MUST be encrypted when copied to persistent
- 244 store.
- 245 ● urn:liberty:names:1.0:igf:pri:retention:nolog
- 246 ○ Indicates that the data value MUST NOT be written to log.

247 2.4.1. LifetimeConstraint

248 The time period for which data MAY be retained for active use by the requestor.

```
249 <element name="LifeTimeConstraint">
250    <complexType>
251      <choice>
252        <sequence>
253          <element name="Minutes" type="int"/>
254          <element name="Hours" type="int"/>
255        </sequence>
256        <sequence>
257          <element name="StartTime" type="dateTime"/>
258          <element name="EndTime" type="dateTime"/>
259        </sequence>
260      </choice>
261      <attribute ref="pri:Issuer"/>
262    </complexType>
263 </element>
```

264 2.5. DataLossOrBreachConstraint

265 Describes the entities (e.g. business or government authority, the user, etc) to be informed if the

266 data is lost or compromised.

```
267 <element name="DataLossOrBreachConstraint">
268    <complexType>
269      <attribute ref="pri:Issuer"/>
270      <attribute name="uri" type="anyURI" use="required"/>
271    </complexType>
272 </element>
```

273 This specification defines two standard URIs for constraining breach reporting.

- 274 • urn:liberty:names:1.0:igf:pri:breachreport:end-user
 - 275 ○ Indicates that the breach MUST be reported to the relevant end-user.
- 276 • urn:liberty:names:1.0:igf:pri:breachreport:source
 - 277 ○ Indicates that the breach MUST be reported to the original source.

278 2.6. ContractOrLegalConstraint

279 Indicates the contractual or legal context governing the sharing of identity attributes.

```
280 <element name="ContractOrLegalConstraint">  
281   <complexType>  
282     <attribute ref="pri:Issuer"/>  
283     <attribute name="uri" type="anyURI" use="required"/>  
284   </complexType>  
285 </element>
```

286 This specification defines a single standard URI for constraining contract or legal context.

- 287 • urn:liberty:names:1.0:igf:pri:contract:context.
 - 288 ○ Indicates that the contractual or legal context under which the data value is
 - 289 sought SHOULD be determined from application context.

290 Our expectation is that communities will define additional URIs based on rules for industry
291 verticals and national jurisdictions.

292 2.7. DataMaskConstraint

293 Describes components of string data which should be masked when data is displayed or logged.

```
294 <element name="DataMaskConstraint">  
295   <complexType>  
296     <attribute ref="pri:Issuer"/>  
297     <attribute name="Pattern" type="string" use="required"/>  
298   </complexType>  
299 </element>
```

300 | **3. References**

301 | RFC2119] S. Bradner, Key words for use in RFCs to Indicate Requirement Levels, IETF RFC
302 | 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>

303 | [S-Policy] Web Services Policy 1.5 Framework, October 2007.
304 | <http://www.w3.org/TR/2004/REC-xmlschema-1-20041028>

305 | [CARML] Phil Hunt (Editor), Liberty Client Attribute Requirements Markup Language
306 | (CARML) Specification, FINAL v1.0, 15 July 2009, Liberty Alliance, available from:
307 | **INSERT LINK HERE ONCE POSTED**

Deleted: ¶
¶
¶
-----Page Break-----

Comment [jb1]: I will add this before posting the doc