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.

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

94 # Contents

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.

```
[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>
```

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.

155 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

161 1.3 References

162 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

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:deployed	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: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:

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

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 indicates 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:defini
     tion"
[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"/>
```