Liberty Alliance Privacy Constraints Specification

Version 1.0

Editors:
Paul Madsen, NTT

Contributors:
Prateek Mishra, Oracle

Abstract:

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

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

NOTICE:

(HIMSS), Helsinki Institute of Physics, Jeff Hodges, Hongkong Post, Guy Huntington, Imprivata, 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

79 ## Contents

Deleted: 1
Deleted: 2
Deleted: 3
Deleted: 3
Deleted: 4
Deleted: 4
Deleted: 4
Deleted: 4
Deleted: 5
Deleted: 5
Deleted: 6
Deleted: 6
Deleted: 6
Deleted: 6
Formatted: Font: (Default) Times New Roman, Underline, Font color: Blue

94

1. Introduction

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

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

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

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

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

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

1.1. Example

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

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

```
7:                Issuer="urn:liberty:names:1.0:igf:pri:entity:user">
8:                ref="urn:liberty:names:1.0:igf:pri:propagate:requestor"/>
9:             <pri:RetentionConstraint
10:               Issuer="urn:liberty:names:1.0:igf:pri:entity:user">
11:               ref="urn:liberty:names:1.0:igf:pri:retention:transient"
12:                     <pri:LifetimeConstraint>
13:                             <pri:Minutes>59</pri:Minutes>
14:                             <pri:Hours>23</pri:Hours>
15:                     </pri:LifetimeConstraint>
16:            </pri:RetentionConstraint>
17:     <wsp:All>
18:</wsp:Policy>
```

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

[a3]-[a5] indicate the purpose for which data is released. [a6]-[a8] indicate that the data items should 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 should be cached in memory for a maximum period of 23 hours and 59 minutes.

1.2. Namespaces

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:

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

1.3. 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].

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.

Formatted: Normal, Don't suppress line numbers

Deleted: ¶

Deleted: ¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶

2. Privacy Constraints

2.1. Attributes

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

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

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

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

2.2. PurposeConstraint

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

```
<element name="PurposeConstraint">
      <complexType>
            <attribute ref="pri:Issuer"/>
            <attribute name="uri" type="anyURI" use="required"/>
      </complexType>
 </element>
```

This specification defines a single standard URI for constraining purpose.

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

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

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

2.3. PropagateConstraint

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

```
<element name="PropagateConstraint">
      <complexType>
            <attribute ref="pri:Issuer"/>
            <attribute name="uri" type="anyURI" use="required"/>
      </complexType>
 </element>
```

This specification defines a single standard URI for constraining propagation.

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

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

2.4. RetentionConstraint

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

```
<element name="RetentionConstraint">
      <complexType>
             <attribute ref="pri:Issuer"/>
             <attribute name="uri" type="anyURI" use="required"/>
       </complexType>
 </element>
```

This specification defines five standard URIs for constraining retention.

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

- Indicates that the data value MAY be persisted.

- urn:liberty:names:1.0:igf:pri:retention:persist:encrypt
  - Indicates that the data value MUST be encrypted when copied to persistent store.

- urn:liberty:names:1.0:igf:pri:retention:nolog
  - Indicates that the data value MUST NOT be written to log.

2.4.1. LifetimeConstraint

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

```
<element name="LifeTimeConstraint">
      <complexType>
            <choice>
                  <sequence>
                        <element name="Minutes" type="int"/>
                        <element name="Hours" type="int"/>
                  </sequence>
                  <sequence>
                        <element name="StartTime" type="dateTime"/>
                        <element name="EndTime" type="dateTime"/>
                  </sequence>
            </choice>
            <attribute ref="pri:Issuer"/>
      </complexType>
</element>
```

2.5. DataLossOrBreachConstraint

Describes the entities (e.g. business or government authority, the user, etc) to be informed if the data is lost or compromised.

```
<element name="DataLossOrBreachConstraint">
      <complexType>
            <attribute ref="pri:Issuer"/>
            <attribute name="uri" type="anyURI" use="required"/>
      </complexType>
</element>
```

This specification defines two standard URIs for constraining breach reporting.

- urn:liberty:names:1.0:igf:pri:breachreport:end-user
    - Indicates that the breach MUST be reported to the relevant end-user.
- urn:liberty:names:1.0:igf:pri:breachreport:source
    - Indicates that the breach MUST be reported to the original source.

2.6. ContractOrLegalConstraint

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

```
<element name="ContractOrLegalConstraint">
       <complexType>
            <attribute ref="pri:Issuer"/>
            <attribute name="uri" type="anyURI" use="required"/>
      </complexType>
</element>
```

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

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

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

2.7. DataMaskConstraint

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

```
<element name="DataMaskConstraint">
      <complexType>
            <attribute ref="pri:Issuer"/>
            <attribute name="Pattern" type="string" use="required"/>
      </complexType>
</element>
```

3. References

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

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

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

Deleted: ¶
¶
¶
Page Break

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