1

OASIS Service Provisioning Markup Language (SPML) v2 - DSML v2 Profile

2
3

OASIS Standard
2006 April 1

4
5

6 Document identifier: pstc-spml2-dsml-profile-os.pdf

7 Location: http://www.oasis-open.org/committees/provision/docs/

8 Send comments to: pstc-comment@lists.oasis-open.org

9 Editor:

10   Jeff Bohren, BMC (Jeff_Bohren@bmc.com)

11

12 Contributors:

13   Robert Boucher, CA
14   Doron Cohen, BMC
15   Gary Cole, Sun Microsystems
16   Cal Collingham, CA
17   Rami Elron, BMC
18   Marco Fanti, Thor Technologies
19   Ian Glazer, IBM
20   James Hu, HP
21   Ron Jacobsen, CA
22   Jeff Larson, Sun Microsystems
23   Hal Lockhart, BEA
24   Prateek Mishra, Oracle Corporation
25   Martin Raepple, SAP
26   Darran Rolls, Sun Microsystems
27   Kent Spaulding, Sun Microsystems
28   Gavenraj Sodhi, CA
29   Cory Williams, IBM
30   Gerry Woods, SOA Software

31

32 Abstract:

33   This specification defines usage of DSML v2 as a data model (profile) for SPML v2.

34 Status:

35   This is an OASIS Standard document produced by the Provisioning Services Technical
36   Committee. It was approved by the OASIS membership on 1 April 2006.

37   If you are on the provision list for committee members, send comments there. If you are not
38   on that list, subscribe to the provision-comment@lists.oasis-open.org list and send
39   comments there. To subscribe, send an email message to provision-comment-
40   request@lists.oasis-open.org with the word "subscribe" as the body of the message.

41   Copyright (C) OASIS Open 2006. All Rights Reserved.

Table of contents

81

82 1. Introduction (non-normative)

83 1.1. Concepts

84   SPML Version 2 (SPMLv2) defines a core protocol **[SPMLv2]** over which different data models can
85   be used to define the actual provisioning data. The combination of a data model with the SPML
86   core specification is referred to as a profile. The use of SPML requires that a specific profile is
87   used, although the choice of which profile is used to negatioted out-of-band by the participating
88   parties.

89   This document describes the use of the DSML protocol as a data model for SPML based
90   provisioning. This profile is optional.

91 1.1.1. DSML Protocol

92   The DSML v2 protocol **[DSMLV2]** was designed to perform LDAP type operations using web
93   services. The DSML V2 protocol defines synchronous request/response semantics and a data
94   model based on attribute/value pairs. DSML V2 does not define an attribute/value pairs schema
95   mechanism.

96 1.1.2. Schema

97   The DSML v2 standard does not define a schema mechanism. A schema mechanism is defined as
98   part of this binding.

99 1.2. Terminology

100   Within this document:
101   - The term "requestor" always refers to a Requesting Authority (RA).
102   - The term "provider" always refers to a Provisioning Service Provider (PSP).
103   - The term "target" always refers to a Provisioning Service Target (PST).
104   - The term "object" (unless otherwise qualified) refers to a Provisioning Service Object (PSO).
105   - The term "client" (unless otherwise qualified) refers to a Requesting Authority (RA).
106   - The term "server" (unless otherwise qualified) refers to a Provisioning Service Provider (PSP).

107 2. Notation

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

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

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

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

119 This specification uses the following typographical conventions in text:

Format	Description	Indicates
`attributeName`	monospace font with *first letter lower-cased*	The name of an XML *attribute*.
`SPMLElementName`	monospace font with *first letter capitalized*	The name of an XML *element* that is defined as part of SPMLv2.
`ns:ForeignElementName`	monospace font *with namespace prefix*	The name of an XML element that is *defined by another specification.*
`<SPMLElement>`	monospace font *surrounded by <>*	*An instance of an XML element* that is defined as part of SPMLv2.
`<ns:ForeignElement>`	monospace font *with namespace prefix* surrounded by <>	An instance of an XML element that is *defined by another specification*.

120 Terms in ***italic bold-face*** are intended to have the meaning defined in the Glossary.

121 Listings of SPML schemas appear like this.

122

123 Example code listings appear like this.

124 Conventional XML namespace prefixes are used throughout the listings in this specification to
125 stand for their respective namespaces as follows, whether or not a namespace declaration is
126 present in the example:
127 - The prefix `dsml:` stands for the Directory Services Markup Language namespace **[DSML].**
128 - The prefix `saml:` stands for the SAML assertion namespace [**SAML**].
129 - The prefix `ds:` stands for the W3C XML Signature namespace [**DS**].
130 - The prefix `xsd:` stands for the W3C XML Schema namespace [**XS**].

131 3. Overview (non-normative)

132 3.1. DSML PSOs

133 A PSO is represented in this binding by a set of attribute/values pairs that is associated with a
134 target-unique identifier. All PSOs are categorized by one or more object classes. The object class
135 for a given PSO is denotes by an attribute named with the reserved name of "objectclass".

3.1.1. PSO Identifier

The PSO Identifier may be an X.509 Distinguished Name (DN), or any identifier that is unique for the target..

```
<spml:pso xmlns:spml="urn:oasis:names:tc:SPML:2:0">
   <spml:psoId  ID="CN=John Doe,OU=accounting,DC=acme.com" targetID="acme.com"/>
</spml:pso>
```

3.1.2. PSO Data

The PSO Data element contains dsml:attr elements, as defined in **[DSML]**. Additional data may be included via the Open Content Model.

```
<spml:pso xmlns:spml="urn:oasis:names:tc:SPML:2:0" >
   <spml:data>
      <attr name="cn" xmlns="urn:oasis:names:tc:DSML:2:0:core">
         <value>John Doe</value>
      </attr>
      <attr name="uid">
         <value>jdoe</value>
      </attr>
      <attr name="email" xmlns="urn:oasis:names:tc:DSML:2:0:core">
         <value>jdoe@acme.com</value>
      </attr>
      <attr name="objectclass" xmlns="urn:oasis:names:tc:DSML:2:0:core">
         <value>user</value>
      </attr>
   </spml:data>
</spml:pso>
```

3.2. Schema

The schema defines the allowed attributes and object classes.

```
<spml:schema xmlns:spml="urn:oasis:names:tc:SPML:2:0"
xmlns:spmldsml="urn:oasis:names:tc:SPML:2:0:DSML">
   <spmldsml:schema>
      <spmldsml:attributeDefinition name="cn" description="Common Name" />
      <spmldsml:attributeDefinition name="uid" description="User ID" />
      <spmldsml:attributeDefinition name="email" description="Email Address" />
      <spmldsml:objectClassDefinition name="person">
        <spmldsml:memberAttributes>
                   <spmldsml:memberAttributes  name="cn"  required="true" />
                   <spmldsml:memberAttributes  name="uid"/>
                   <spmldsml:memberAttributes  name="email"/>
              </spmldsml:memberAttributes>
      </spmldsml:objectClassDefinition>
   </spmldsml:schema>
</spml:schema>
```

3.3. Core Operations

3.3.1. Add Request

The Add Request creates PSOs. The Add Request must contain a <data> element that contains DSML v2 <attr> elements that define the new PSO. The Add Request may also pass a PSO

182 Identifier (<psoID> element), a container PSO ID (<containerID> element), or a target ID
183 (<targetID> element). If a PSO identifier is not defined in the Add Request, the new PSO Identifier
184 must be returned in the Add Response.

```
185  <spml:addRequest xmlns:spml="urn:oasis:names:tc:SPML:2:0">
186     <spml:containerID  ID="OU=accounting,DC=acme.com" targetID="acme.com "/>
187     <spml:data>
188        <attr name="CN" xmlns="urn:oasis:names:tc:DSML:2:0:core">
189           <value> John Doe </value>
190        </attr>
191        <attr name="uid" xmlns="urn:oasis:names:tc:DSML:2:0:core">
192           <value>jdoe</value>
193        </attr>
194        <attr name="objectclass" xmlns="urn:oasis:names:tc:DSML:2:0:core">
195           <value>user</value>
196        </attr>
197     </spml:data>
198  </spml:addRequest>
```

3.3.2.   Add Response

200 The Add Response message will contain the new PSO ID (unless it was specified in the Add
201 Request). If the creation of the new PSO resulted in attributes being adding or modified in the new
202 PSO, the entire PSO Data should be returned in the response.

```
203  <spml:addResponse status="spml:success" xmlns:spml="urn:oasis:names:tc:SPML:2:0">
204     <spml:psoId ID="CN=John Doe,OU=accounting,DC=acme.com" targetID="acme.com "/>
205     <spml:data>
206        <attr name="CN" xmlns="urn:oasis:names:tc:DSML:2:0:core">
207           <value> John Doe </value>
208        </attr>
209        <attr name="uid" xmlns="urn:oasis:names:tc:DSML:2:0:core">
210           <value>jdoe</value>
211        </attr>
212        <attr name="email" xmlns="urn:oasis:names:tc:DSML:2:0:core">
213           <value>jdoe@acme.com</value>
214        </attr>
215        <attr name="objectclass" xmlns="urn:oasis:names:tc:DSML:2:0:core">
216           <value>user</value>
217        </attr>
218     </spml:data>
219  </spml:addResponse>
```

3.3.3.   Modify Request

221 The Modify Request modifies the specified PSO. The Modify Request must always contain the
222 PSO Identifier.

```
223  <spml:modifyRequest xmlns:spml="urn:oasis:names:tc:SPML:2:0">
224     <spml:psoId ID="CN=John Doe,OU=accounting,DC=acme.com" targetID="acme.com "/>
225     <spml:modification>
226       <modification name ="CN" operation ="replace"
227  xmlns="urn:oasis:names:tc:DSML:2:0:core">
228          <value>Jane Doe</value>
229       </modification>
230     </spml:modification>
231  </spml:modifyRequest >
```

3.3.4. Modify Response

If the Modify Request causes the PSO ID to change, then the Modify Response must contain the new PSO ID.

```
<spml:modifyResponse status="spml:success"
xmlns:spml="urn:oasis:names:tc:SPML:2:0">
   <spml:psoId ID="CN=Jane Doe,OU=accounting,DC=acme.com" targetID="acme.com "/>
</spml:modifyResponse>
```

3.3.5. Delete Request

The Delete Request deletes a specified PSO.

```
<spml:deleteRequest xmlns:spml="urn:oasis:names:tc:SPML:2:0">
   <spml:psoId ID="CN=John Doe,OU=accounting,DC=acme.com" targetID="acme.com "/>
</spml:deleteRequest >
```


3.3.6. Lookup Request

The Lookup Request is used to retrieve the data for a specified PSO.

```
<spml:lookupRequest xmlns:spml="urn:oasis:names:tc:SPML:2:0">
   <spml:psoId ID="CN=John Doe,OU=accounting,DC=acme.com" targetID="acme.com "/>
</spml:lookupRequest>
```

3.3.7. Lookup Response

The Lookup Response contains the retrieved PSO data.

```
<spml:lookupResponse status="spml:success"
xmlns:spml="urn:oasis:names:tc:SPML:2:0">
   <spml:psoId ID="CN=John Doe,OU=accounting,DC=acme.com" targetID="acme.com "/>
   <spml:data>
      <attr name="CN" xmlns="urn:oasis:names:tc:DSML:2:0:core">
         <value> John Doe </value>
      </attr>
      <attr name="uid" xmlns="urn:oasis:names:tc:DSML:2:0:core">
         <value>jdoe</value>
      </attr>
      <attr name="email" xmlns="urn:oasis:names:tc:DSML:2:0:core">
         <value>jdoe@acme.com</value>
      </attr>
      <attr name="objectclass" xmlns="urn:oasis:names:tc:DSML:2:0:core">
         <value>user</value>
      </attr>
   </spml:data>
</spml:lookupResponse>
```

3.4. Search Operations

If the Search Capability is supported, the DSML filters and attribute declarations should be used to scope the results of the search.

3.4.1. Search Request

The search request can specify DSML filters and attribute declarations, as defined in **[DSML]**.

```
<spmlsearch:searchRequest xmlns:spml="urn:oasis:names:tc:SPML:2:0"
xmlns:spmlsearch="urn:oasis:names:tc:SPML:2:0:search">
    <spmlsearch:query scope = "spmlsearch:oneLevel">
        <spml:basePSOID ID="CN=John Doe,OU=accounting,DC=acme.com"
targetID="acme.com" />
        <filter xmlns="urn:oasis:names:tc:DSML:2:0:core">
            <substrings name = "cn">
                <initial>John</initial>
            </substrings>
        </filter>
        <attributes xmlns="urn:oasis:names:tc:DSML:2:0:core">
            <attribute name = "cn" />
            <attribute name = "email" />
        </attributes>
    </spmlsearch:query>
</spmlsearch:searchRequest>
```

3.4.2. Search Response

```
<spmlsearch:searchResponse status="spml:success"
xmlns:spml="urn:oasis:names:tc:SPML:2:0"
xmlns:spmlsearch="urn:oasis:names:tc:SPML:2:0:search">
    <spml:pso>
        <spml:psoId ID="CN=John Doe,OU=accounting,DC=acme.com"
targetID="acme.com"/>
        <spml:data>
            <attr name="cn" xmlns="urn:oasis:names:tc:DSML:2:0:core">
                <value>John Doe</value>
            </attr>
            <attr name="email" xmlns="urn:oasis:names:tc:DSML:2:0:core">
                <value>jdoe@acme.com</value>
            </attr>
        </spml:data>
    </spml:pso>
    <spml:pso>
        <spml:psoId ID="CN=John Smith,OU=accounting,DC=acme.com"
targetID="acme.com"/>
        <spml:data>
            <attr name="cn" xmlns="urn:oasis:names:tc:DSML:2:0:core">
                <value>John Smith</value>
            </attr>
            <attr name="email" xmlns="urn:oasis:names:tc:DSML:2:0:core">
                <value>jsmith@acme.com</value>
            </attr>
        </spml:data>
    </spml:pso>
</spmlsearch:searchResponse>
```

4. Specification (Normative)

4.1. Namespaces

The DSMLv2 Profile uses the DSML v2 namespace which is defined as:

```
urn:oasis:names:tc:DSML:2:0:core
```

The specification uses the prefix dsml: to refer to this namespace.

The DSMLv2 Profile defines some elements that are specific to the profile. The namespace for the profile itself is defined as:

```
urn:oasis:names:tc:SPML:2:0:DSML
```

The specification uses the prefix spmldsml: to refer to this namespace.

4.2. Core Capability

4.2.1. Element <spml:data>

The *<spml:data>* element MUST contain zero or many *<dsml:attr>* elements.

4.2.2. Element <spml:modification>

The *<spml:modification>* element MUST contain zero or many *<dsml:modification>* elements. The "modificationType" on the *<spml:modification>* MUST NOT be specified since the *<dsml:modification>* defines the modification type.

4.2.3. Element <spml:schema>

If the schema is defined in-band, the *<spml:schema>* element MUST contain one or more *<spmldsml:schema>* elements. If the schema is define out-of-band, the "ref" attribute on the *<spml:schema>* element MUST be set to the URN of the referenced schema.

If ony a subset of the object classes defined in the schema are supported for the target, then the *<spml:schema>* element MUST include *<spml:supportedSchemaEntity>*. If no *<spml:supportedSchemaEntity>* are defined in the *<spml:schema>* element, then it is assumed are object classes are supported by the target.

4.2.4. Element <supportedSchemaEntity>

The "entityName" attribute on the *<spml:supportedSchemaEntity>* element MUST refer only to object classes defined in the referenced schema. All attributes on the referenced object classes are assumed to be supported.

4.3. Search Capability

4.3.1. Element <spmlsearch:query>

The *<spmlsearch:query>* element MAY contain *<dsml:filter>* and *<dsml:attributes>* to filter the results of the search.

4.4. DSML Profile Schema

4.4.1. Element <spmldsml:schema>

The *<spmldsml:schema>* element defines the DSML schema for the target. The *<spmldsml:schema>* element contains zero or more *<spmldsml:objectClassDefinition>* elements and zero or more *<spmldsml:attributeDefinition>* elements.

4.4.2. Element <spmldsml:objectClassDefinition>

The *<spmldsml:objectClassDefinition>* element defines DSML v2 object classes supported by the target. The *<spmldsml:objectClassDefinition>* element contains zero or more *<spmldsml:memberAttributes>* elements which define the attributes that may be included on objects of the specified object class. The *<spmldsml:objectClassDefinition>* element contains zero or more <spmldsml:superiorClasses> which define the superior object classes to the specified object class.

4.4.3. Element <spmldsml:attributeDefinition>

The *<spmldsml:attributeDefinition>* element defines DSML v2 attributes supported by the target. The *<spmldsml:attributeDefinition>* element has the following attributes:

- description – textual description of the attribute

- multivalued – true if the attribute is multivalued, false if it is single valued

- type – attribute syntax

- name – attribute name (e.g. "cn")

.

Appendix A. References

[AES]   National Institute of Standards and Technology (NIST), FIPS-197: Advanced Encryption Standard, **http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf**, National Institute of Standards and Technology (NIST)

[ARCHIVE-1]   OASIS Provisioning Services Technical Committee, email archive, **http://www.oasis-open.org/apps/org/workgroup/provision/email/archives/index.html**, OASIS PS-TC

[DS]   IETF/W3C, *W3C XML Signatures*, **http://www.w3.org/Signature/**, W3C/IETF

[DSML]   OASIS Directory Services Markup Standard, *DSML V2.0 Specification*, **http://www.oasis-open.org/specs/index.php#dsmlv2**, OASIS DSML Standard

[GLOSSARY]   OASIS Provisioning Services TC, *Glossary of Terms*, **http://www.oasis-open.org/apps/org/workgroup/provision/download.php**, OASIS PS-TC

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

[RFC 2246]   T. Dierks and C. Allen, *The TLS Protocol*, **http://www.ietf.org/rfc/rfc2246.txt**, IETF

[SAML]   OASIS Security Services TC, **http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security**, OASIS SS-TC

[SOAP]   W3C XML Protocol Working Group, **http://www.w3.org/2000/xp/Group/**

[SPML-Bind]   OASIS Provisioning Services TC, SPML V1.0 Protocol Bindings, **http://www.oasis-open.org/apps/org/workgroup/provision/download.php/1816/draft-pstc-bindings-03.doc**, OASIS PS-TC

[SPML-REQ]   OASIS Provisioning Services Technical Committee, *Requirements*, **http://www.oasis-open.org/apps/org/workgroup/provision/download.php/2277/draft-pstc-requirements-01.doc**, OASIS PS-TC

[SPML-UC]   OASIS Provisioning Services Technical Committee, *SPML V1.0 Use Cases*, **http://www.oasis-open.org/apps/org/workgroup/provision/download.php/988/drfat-spml-use-cases-05.doc**, OASIS PS-TC

[SPMLv2-Profile-DSML]   OASIS Provisioning Services Technical Committee, SPMLv2 DSMLv2 Profile, OASIS PS-TC

[SPMLv2-Profile-XSD]   OASIS Provisioning Services Technical Committee, SPML V2 XSD Profile, OASIS PS-TC

[SPMLv2-REQ]   OASIS Provisioning Services Technical Committee, Requirements, OASIS PS-TC

418 **[SPMLv2-ASYNC]** OASIS Provisioning Services Technical Committee, XML Schema
419 Definitions for Async Capability of SPMLv2, OASIS PS-TC

420 **[SPMLv2-BATCH]** OASIS Provisioning Services Technical Committee, XML Schema
421 Definitions for Batch Capability of SPMLv2, OASIS PS-TC

422 **[SPMLv2-BULK]** OASIS Provisioning Services Technical Committee, XML Schema
423 Definitions for Bulk Capability of SPMLv2, OASIS PS-TC

424 **[SPMLv2-CORE]** OASIS Provisioning Services Technical Committee, XML Schema
425 Definitions for Core Operations of SPMLv2, OASIS PS-TC

426 **[SPMLv2-PASS]** OASIS Provisioning Services Technical Committee, XML Schema
427 Definitions for Password Capability of SPMLv2, OASIS PS-TC

428 **[SPMLv2-REF]** OASIS Provisioning Services Technical Committee, XML Schema
429 Definitions for Reference Capability of SPMLv2, OASIS PS-TC

430 **[SPMLv2-SEARCH]** OASIS Provisioning Services Technical Committee, XML Schema
431 Definitions for Search Capability of SPMLv2, OASIS PS-TC

432 **[SPMLv2-SUSPEND]** OASIS Provisioning Services Technical Committee, XML Schema
433 Definitions for Suspend Capability of SPMLv2, OASIS PS-TC

434 **[SPMLv2-UPDATES]** OASIS Provisioning Services Technical Committee, XML Schema
435 Definitions for Updates Capability of SPMLv2, OASIS PS-TC

436 **[SPMLv2-UC]** OASIS Provisioning Services Technical Committee., SPML V2.0 Use
437 Cases, OASIS PS-TC

438 **[WSS]** OASIS Web Services Security (WSS) TC, **http://www.oasis-**
439 **open.org/committees/tc_home.php?wg_abbrev=wss**, OASIS SS-TC

440 **[X509]** RFC 2459 - Internet X.509 Public Key Infrastructure Certificate and CRL
441 Profile, **http://www.ietf.org/rfc/rfc2459.txt**

442 **[XSD]** W3C Schema WG ., *W3C XML Schema*,
443 **http://www.w3.org/TR/xmlschema-1/** W3C

444

445

446

Appendix B. Acknowledgments

The following individuals were voting members of the Provisioning Services committee at the time that this version of the specification was issued:

Jeff Bohren, BMC
Robert Boucher, CA
Gary Cole, Sun Microsystems
Rami Elron, BMC
Marco Fanti, Thor Technologies
James Hu, HP
Martin Raepple, SAP
Gavenraj Sodhi, CA
Kent Spaulding, Sun Microsystems

Appendix C. Notices

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS's procedures with respect to rights in OASIS specifications can be found at the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification, can be obtained from the OASIS Executive Director.

OASIS has been notified of intellectual property rights claimed in regard to some or all of the contents of this specification. For more information consult the online list of claimed rights.

OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to implement this specification. Please address the information to the OASIS Executive Director.