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

Committee Draft 1.0
2005 September 14

Location: http://www.oasis-open.org/committees/provision/docs/
Send comments to: pstc-comment@lists.oasis-open.org
Editor: Jeff Bohren, BMC (Jeff_Bohren@bmc.com)

Contributors:
Robert Boucher, CA
Doron Cohen, BMC
Gary Cole, Sun Microsystems
Cal Collingham, CA
Rami Elron, BMC
Marco Fanti, Thor Technologies
Ian Glazer, IBM
James Hu, HP
Ron Jacobsen, CA
Jeff Larson, Sun Microsystems
Hal Lockhart, BEA
Prateek Mishra, Oracle Corporation
Martin Raepple, SAP
Darran Rolls, Sun Microsystems
Kent Spaulding, Sun Microsystems
Gavenraj Sodhi, CA
Cory Williams, IBM
Gerry Woods, SOA Software

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

This is a candidate Committee Specification that is undergoing a vote of the OASIS membership in pursuit of OASIS Standard status.

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

Copyright (C) OASIS Open 2005. All Rights Reserved.
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.</td>
<td>Concepts</td>
<td>4</td>
</tr>
<tr>
<td>1.1.1.</td>
<td>DSML Protocol</td>
<td>4</td>
</tr>
<tr>
<td>1.1.2.</td>
<td>Schema</td>
<td>4</td>
</tr>
<tr>
<td>1.2.</td>
<td>Terminology</td>
<td>4</td>
</tr>
<tr>
<td>2.</td>
<td>Notation</td>
<td>4</td>
</tr>
<tr>
<td>3.</td>
<td>Overview (non-normative)</td>
<td>5</td>
</tr>
<tr>
<td>3.1.</td>
<td>DSML PSOs</td>
<td>5</td>
</tr>
<tr>
<td>3.1.1.</td>
<td>PSO Identifier</td>
<td>6</td>
</tr>
<tr>
<td>3.1.2.</td>
<td>PSO Data</td>
<td>6</td>
</tr>
<tr>
<td>3.2.</td>
<td>Schema</td>
<td>6</td>
</tr>
<tr>
<td>3.3.</td>
<td>Core Operations</td>
<td>7</td>
</tr>
<tr>
<td>3.3.1.</td>
<td>Add Request</td>
<td>7</td>
</tr>
<tr>
<td>3.3.2.</td>
<td>Add Response</td>
<td>7</td>
</tr>
<tr>
<td>3.3.3.</td>
<td>Modify Request</td>
<td>7</td>
</tr>
<tr>
<td>3.3.4.</td>
<td>Delete Request</td>
<td>8</td>
</tr>
<tr>
<td>3.3.5.</td>
<td>Lookup Request</td>
<td>8</td>
</tr>
<tr>
<td>3.3.6.</td>
<td>Lookup Response</td>
<td>8</td>
</tr>
<tr>
<td>3.4.</td>
<td>Search Operations</td>
<td>9</td>
</tr>
<tr>
<td>3.4.1.</td>
<td>Search Request</td>
<td>9</td>
</tr>
<tr>
<td>3.4.2.</td>
<td>Search Response</td>
<td>9</td>
</tr>
<tr>
<td>4.</td>
<td>Specification (Normative)</td>
<td>10</td>
</tr>
<tr>
<td>4.1.</td>
<td>Namespaces</td>
<td>10</td>
</tr>
<tr>
<td>4.2.</td>
<td>Core Capability</td>
<td>10</td>
</tr>
<tr>
<td>4.2.1.</td>
<td>Element <a href="">spml:data</a></td>
<td>10</td>
</tr>
<tr>
<td>4.2.2.</td>
<td>Element <a href="">spml:modification</a></td>
<td>10</td>
</tr>
<tr>
<td>4.2.3.</td>
<td>Element <a href="">spml:schema</a></td>
<td>10</td>
</tr>
<tr>
<td>4.2.4.</td>
<td>Element &lt;supportedSchemaEntity&gt;</td>
<td>10</td>
</tr>
<tr>
<td>4.3.</td>
<td>Search Capability</td>
<td>11</td>
</tr>
<tr>
<td>4.3.1.</td>
<td>Element <a href="">spmlsearch:query</a></td>
<td>11</td>
</tr>
<tr>
<td>4.4.</td>
<td>DSML Profile Schema</td>
<td>11</td>
</tr>
<tr>
<td>4.4.1.</td>
<td>Element <a href="">spmldsml:schema</a></td>
<td>11</td>
</tr>
<tr>
<td>4.4.2.</td>
<td>Element <a href="">spmldsml:objectClassDefinition</a></td>
<td>11</td>
</tr>
<tr>
<td>4.4.3.</td>
<td>Element <a href="">spmldsml:attributeDefinition</a></td>
<td>11</td>
</tr>
<tr>
<td>Appendix A</td>
<td>References</td>
<td>12</td>
</tr>
</tbody>
</table>
1. Introduction (non-normative)

1.1. Concepts

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

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

1.1.1. DSML Protocol

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

1.1.2. Schema

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

1.2. Terminology

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

2. 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.

This specification uses the following typographical conventions in text:

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
<th>Indicates</th>
</tr>
</thead>
<tbody>
<tr>
<td>attributeName</td>
<td>monospace font with first letter lower-cased</td>
<td>The name of an XML attribute.</td>
</tr>
<tr>
<td>SPMLElementName</td>
<td>monospace font with first letter capitalized</td>
<td>The name of an XML element that is defined as part of SPMLv2.</td>
</tr>
<tr>
<td>ns:ForeignElementName</td>
<td>monospace font with namespace prefix</td>
<td>The name of an XML element that is defined by another specification.</td>
</tr>
<tr>
<td>&lt;SPMLElement&gt;</td>
<td>monospace font surrounded by &lt;&gt;</td>
<td>An instance of an XML element that is defined as part of SPMLv2.</td>
</tr>
<tr>
<td><a href="">ns:ForeignElement</a></td>
<td>monospace font with namespace prefix surrounded by &lt;&gt;</td>
<td>An instance of an XML element that is defined by another specification.</td>
</tr>
</tbody>
</table>

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

Listings of SPML schemas appear like this.

Example code listings appear like this.

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

- The prefix dsml: stands for the Directory Services Markup Language namespace [DSML].
- The prefix saml: stands for the SAML assertion namespace [SAML].
- The prefix ds: stands for the W3C XML Signature namespace [DS].
- The prefix xsd: stands for the W3C XML Schema namespace [XS].

3. Overview (non-normative)

3.1. DSML PSOs

A PSO is represented in this binding by a set of attribute/values pairs that is associated with a target-unique identifier. All PSOs are categorized by one or more object classes. The object class 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.

```xml
<spml:pso>
    <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.

```xml
<spml:pso>
    ...
    <spml:data>
        <attr name="cn">
            <value>John Doe</value>
        </attr>
        <attr name="uid">
            <value>jdoe</value>
        </attr>
        <attr name="email">
            <value>jdoe@acme.com</value>
        </attr>
        <attr name="objectclass">
            <value>user</value>
        </attr>
    </spml:data>
</spml:pso>
```

3.2. Schema

The schema defines the allowed attributes and object classes.

```xml
<spml:schema>
    <spml:objectClassDefinition name="person">
        <spml:memberAttributes>
            <spml:memberAttributes name="cn" required="true"/>
            <spml:memberAttributes name="uid"/>
            <spml:memberAttributes name="email"/>
        </spml:memberAttributes>
    </spml:objectClassDefinition>
</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 Identifier (<psoID> element), a container PSO ID (<containerID> element), or a target ID (<targetID> element). If a PSO identifier is not defined in the Add Request, the new PSO Identifier must be returned in the Add Response.

```xml
<spml:addRequest>
  <spml:containerID ID = "OU=accounting,DC=acme.com" targetID = "acme.com"/>
  <spml:data>
    <attr name="CN">
      <value>John Doe</value>
    </attr>
    <attr name="uid">
      <value>jdoe</value>
    </attr>
    <attr name="objectclass">
      <value>user</value>
    </attr>
  </spml:data>
</spml:addRequest>
```

3.3.2. Add Response

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

```xml
<spml:addResponse status = "success">
  <spml:psoId ID="CN=John Doe,OU=accounting,DC=acme.com" targetID="acme.com"/>
  <spml:data>
    <attr name="CN">
      <value>John Doe</value>
    </attr>
    <attr name="uid">
      <value>jdoe</value>
    </attr>
    <attr name="email">
      <value>jdoe@acme.com</value>
    </attr>
    <attr name="objectclass">
      <value>user</value>
    </attr>
  </spml:data>
</spml:addResponse>
```

3.3.3. Modify Request

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

```xml
<spml:modifyRequest>
  <spml:psoId ID="CN=John Doe,OU=accounting,DC=acme.com" targetID="acme.com"/>
  <spml:modification>
    <modification name ="CN" operation ="replace">
      <attr name="CN">
        <value>John Doe</value>
      </attr>
    </modification>
  </spml:modification>
</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.

```xml
<spml:modifyResponse status = "success">
  <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.

```xml
<spml:deleteRequest>
  <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.

```xml
<spml:lookupRequest>
  <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.

```xml
<spml:lookupResponse status = "success">
  <spml:psoId ID="CN=John Doe,OU=accounting,DC=acme.com" targetID="acme.com "/>
  <spml:data>
    <attr name="CN">
      <value> John Doe </value>
    </attr>
    <attr name="uid">
      <value>jdoe</value>
    </attr>
    <attr name="email">
      <value>jdoe@acme.com</value>
    </attr>
    <attr name="objectclass">
      <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].

```xml
<spmlsearch:searchRequest>
  <spmlsearch:query scope = "spmlsearch:oneLevel">
    <spml:basePSOID ID="CN=John Doe,OU=accounting,DC=acme.com" targetID="acme.com">
      <dsml:filter>
        <dsml:substrings name = "cn">
          <dsml:initial>John</dsml:initial>
        </dsml:substrings>
      </dsml:filter>
      <dsml:attributes>
        <dsml:attribute name = "cn" />  
        <dsml:attribute name = "email" />
      </dsml:attributes>
    </spml:basePSOID>
  </spmlsearch:query>
</spmlsearch:searchRequest>
```

3.4.2. **Search Response**

```xml
<spml:searchResponse status = " success">
  <spml:pso>
    <spml:psoid ID="CN=John Doe,OU=accounting,DC=acme.com" targetID="acme.com"/>
    <spml:data>
      <dsml:attr name="cn">
        <dsml:value>John Doe</dsml:value>
      </dsml:attr>
      <dsml:attr name="email">
        <dsml:value>jdoe@acme.com</dsml:value>
      </dsml:attr>
    </spml:data>
  </spml:pso>
  <spml:pso>
    <spml:psoid ID="CN=John Smith,OU=accounting,DC=acme.com" targetID="acme.com"/>
    <spml:data>
      <dsml:attr name="cn">
        <dsml:value>John Smith</dsml:value>
      </dsml:attr>
      <dsml:attr name="email">
        <dsml:value>jsmith@acme.com</dsml:value>
      </dsml:attr>
    </spml:data>
  </spml:pso>
</spml: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 spml:dsml: 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 <spml:dsml: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 only 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 <spml:dsml:schema>

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

4.4.2. Element <spml:dsml:objectClassDefinition>

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

4.4.3. Element <spml:dsml:attributeDefinition>

The <spml:dsml:attributeDefinition> element defines DSML v2 attributes supported by the target. The <spml:dsml: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, 

[ARCHIVE-1] OASIS Provisioning Services Technical Committee, email archive, 

[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


[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


[SPML-Bind] OASIS Provisioning Services TC, SPML V1.0 Protocol Bindings, 

[SPML-REQ] OASIS Provisioning Services Technical Committee, Requirements, 

[SPML-UC] OASIS Provisioning Services Technical Committee, SPML V1.0 Use Cases, 

[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
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 implementors or users of this specification, can be obtained from the OASIS President.

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 President.

Copyright © OASIS Open 2005. All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself does not be modified in any way, such as by removing the copyright notice or references to OASIS, except as needed for the purpose of developing OASIS specifications, in which case the procedures for copyrights defined in the OASIS Intellectual Property Rights document must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.