SAML V2.0 Metadata Extensions for Documentation and Registration
Information Version 1.0

Working Draft 01

[24 November 2010]

Technical Committee:
OASIS Security Services TC

Chair(s):
Thomas Hardjono, M.I.T.
Nate Kingenstein, Internet2

Editor(s):
Chad La Joie, Internet2

Related Work:24
This specification defines extensions for use with SAML V2.0 Metadata [SAML2Meta].

Declared XML Namespace(s):
urn:oasis:names:tc:SAML:metadata:dri

Abstract:
This document defines a set of extensions to SAML metadata that provide information about the
creation and intended usage of the metadata document and information about who and how
particular entities were registered.

Status:
This document is a Working Draft and as such as no official standing with regard to the OASIS
Technical Committee Process.

Copyright © OASIS® 2010. All Rights Reserved.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual
Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

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,
distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice
and this section are included on all such copies and derivative works. However, this document itself may
not be modified in any way, including by removing the copyright notice or references to OASIS, except as
needed for the purpose of developing any document or deliverable produced by an OASIS Technical
Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, 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.
# Table of Contents

1 Introduction ........................................................................................................................................... 3  
   1.1 Terminology and Notation ........................................................................................................... 3  
   1.2 Normative References .................................................................................................................. 3  
2 Metadata Extensions for Documentation and Registration Information .............................................. 5  
   2.1 Document Information .................................................................................................................. 5  
      2.1.1 Element `<mddri:DocumentInfo>` ..................................................................................... 5  
      2.1.2 Element `<mddri:UsagePolicy>` ....................................................................................... 6  
      2.1.3 Element `<mddri:PublicationPath>` ................................................................................. 6  
      2.1.4 Element `<mddri:Publication>` ......................................................................................... 7  
   2.2 Registration Information ............................................................................................................... 7  
      2.2.1 Element `<mddri:RegistrationInfo>` ............................................................................... 7  
      2.2.2 Element `<mddri:RegistrationPolicy>` ............................................................................ 8  
   2.3 Example .......................................................................................................................................... 8  
3 Conformance .......................................................................................................................................... 10  
   3.1 SAML V2.0 Metadata Extensions for Documentation and Registration Information Version 1.0 ........ 10
1 Introduction

SAML Metadata [SAML2Meta] provides a mechanism for describing the information necessary for various SAML actors to interact. However, it does not provide basic information which may facilitate the business processes surrounding the production, consumption or use of metadata. For example, when a metadata document was created, when an entity was first registered, etc.

The two extensions defined in this document are informed by the common registration/publication model found in other network architectures (e.g., DNS, PKI). In this case the registrar is an organization will accepts metadata for a particular entity and vouches for some, or all, of the data contained therein. The publisher is responsible for making information, collected by registrars, available, hopefully in a scalable manner, to interested parties.

1.1 Terminology and Notation

The keywords "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 [RFC 2119].

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:

<table>
<thead>
<tr>
<th>Prefix</th>
<th>XML Namespace</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>saml:</td>
<td>urn:oasis:names:tc:SAML:2.0:assertion</td>
<td>This is the SAML V2.0 assertion namespace defined in the SAML V2.0 core specification [SAML2Errata].</td>
</tr>
<tr>
<td>md:</td>
<td>urn:oasis:names:tc:SAML:2.0:metadata</td>
<td>This is the SAML V2.0 metadata namespace defined in the SAML V2.0 metadata specification [SAML2Meta].</td>
</tr>
<tr>
<td>xsd:</td>
<td><a href="http://www.w3.org/2001/XMLSchema">http://www.w3.org/2001/XMLSchema</a></td>
<td>This namespace is defined in the W3C XML Schema specification [Schema1]. In schema listings, this is the default namespace and no prefix is shown.</td>
</tr>
<tr>
<td>xsi:</td>
<td><a href="http://www.w3.org/2001/XMLSchema-instance">http://www.w3.org/2001/XMLSchema-instance</a></td>
<td>This is the XML Schema namespace for schema-related markup that appears in XML instances [Schema1].</td>
</tr>
</tbody>
</table>

This specification uses the following typographical conventions in text: <ns:Element>, Attribute, Datatype, OtherCode.

This specification uses the following typographical conventions in XML listings:

Listings of XML schemas appear like this.

Listings of XML examples appear like this. These listings are non-normative.

1.2 Normative References


2 Metadata Extensions for Documentation and Registration Information

2.1 Document Information

The document information extension is used to denote information about the producer of a metadata document, the sources of other metadata documents which may have been combined, in whole or in part, into the prepared document, and the intended usage of the prepared document.

Such document information may be used for things like uniquely identifying a document when troubleshooting issues (e.g., "I am looking at the document with serial number ABC123...") or as input to trust decisions (e.g., "don’t trust metadata that came through publisher X").

The `<mddri:DocumentInfo>` container element, defined below, MUST appear within the `<md:Extensions>` element of either `<md:EntitiesDescriptor>` or `<md:EntityDescriptor>` elements. The use of `<mddri:DocumentInfo>`, or any other element defined in this section, outside of that context is not defined by this specification.

When the `<mddri:DocumentInfo>` appears in the `<md:Extensions>` element of a `<md:EntitiesDescriptor>` it applies to all descendant `<md:EntitiesDescriptor>` and `<md:EntityDescriptor>` elements.

The `<mddri:DocumentInfo>` element MUST NOT appear more than once within the `<md:Extensions>` element of a given `<md:EntitiesDescriptor>` or `<md:EntityDescriptor>` element.

2.1.1 Element `<mddri:DocumentInfo>`

The `<mddri:DocumentInfo>` element contains information which pertains to the metadata document as a whole. When the `<mddri:DocumentInfo>` element is present within the `<md:Extensions>` element of the document root element either the `<mddri:CreationInstant>` or `<mddri:SerialNumber>` element SHOULD be present.

This element contains the following elements, in any order:

- **creationInstant [Optional]**
  
  The instant the metadata document was created. Creation is loosely defined as the moment when the metadata document is ready for consumption by external processes. This may, for example, correspond to the time a document is signed.

  Time values MUST be expressed in the UTC timezone using the ‘Z’ timezone identifier.

- **serialNumber [Optional]**
  
  A unique, publisher-specific, serial number for this metadata document. This serial number MAY change independently of the ID attribute found on `<md:EntitiesDescriptor>` and `<md:EntityDescriptor>` elements. For example, if a metadata document is auto-generated, the ID attribute may change upon each generation but the SerialNumber may only change if a particular set of data of changes.

  The serial number MUST be considered an opaque string.
A URL to a document providing a human readable description of the intended usage for the metadata document.

There SHOULD NOT be more than one `<mddri:UsagePolicy>`, within a given `<mddri:DocumentInfo>`, for a given language.

A list of publishers of this metadata document.

```xml
<complexType name="DocumentInfoType">
  <sequence>
    <element ref="mddri:UsagePolicy" minOccurs="0" maxOccurs="unbounded"/>
    <element ref="mddri:PublicationPath" minOccurs="0" maxOccurs="1"/>
    <any namespace="##other" processContents="lax"/>
  </sequence>
  <attribute name="creationInstant" type="dateTime"/>
  <attribute name="serialNumber" type="string"/>
  <anyAttribute namespace="##other" processContents="lax"/>
</complexType>
```

### 2.1.2 Element `<mddri:UsagePolicy>`

The `<mddri:UsagePolicy>` element is a URL to a localized description of the intended usage of this metadata document. The URL MUST represent a single, immutable, policy document. Any changes made to an existing policy document MUST result in a new URL. The URL SHOULD resolve to a human readable form of the policy document for the entire period in which the policy may be in use.

```xml
<element name="UsagePolicy" type="md:localizedURIType"/>
```

### 2.1.3 Element `<mddri:PublicationPath>`

The `<mddri:PublicationPath>` element provides a record of the publication path, from current publication to initial publication, for the set of metadata associated with the containing `<mddri:DocumentInfo>` element.

The contained `<mddri:Publication>` element represents one step in the publication path. The list of `<mddri:Publication>` elements is ordered from most recent (the current publication) to least recent (the initial source publication).

For example, assume the current publication is PubC. Further assume that an `<md:EntityDescriptor>` was retrieved from PubB and included in PubC. Also assume that this `<md:EntityDescriptor>` originated in PubA and was included in PubB. In such a situation the publication path for that entity descriptor would be PubC, PubB, PubA.

The publication from which the `<md:EntityDescriptor>` or `<md:EntitiesDescriptor>`, to which this extension is applied, was retrieved.

```xml
<element name="PublicationPath" type="mddri:PublicationPathType"/>
<complexType name="PublicationPathType">
  <sequence>
    <element ref="mddri:Publication" minOccurs="0" maxOccurs="unbounded"/>
  </sequence>
</complexType>
```
2.1.4 Element `<mddri:Publication>`

The `<mddri:Publication>` element identifies a metadata document that was incorporated, in full or in part, into the metadata document containing this extension.

`publisher` [Required]

A unique identifier for the publisher of the metadata. This may be the location from which the metadata was retrieved or an abstracted identifier such as a SAML entity ID.

`creationInstant` [Optional]

The creation instant of the republished `<md:EntitiesDescriptor>` or `<md:EntityDescriptor>` elements, as given by the `<mddri:CreationInstant>` of the first ancestral `<md:EntitiesDescriptor>` or `<md:EntityDescriptor>`.

`serialNumber` [Optional]

The serial number of the republished `<md:EntitiesDescriptor>` or `<md:EntityDescriptor>` elements, as given by the `<mddri:CreationInstant>` of the first ancestral `<md:EntitiesDescriptor>` or `<md:EntityDescriptor>`.

```xml
<complexType name="PublicationType">
  <attribute name="publisherID" type="string" use="required" />
  <attribute name="creationInstant" type="dateTime" />
  <attribute name="serialNumber" type="string" />
</complexType>
```

2.2 Registration Information

The registration information extension is used to provide information about the registrar of an entity. That is, the entity that took in SAML metadata, verified the metadata according to its registration policy, and made the information available to a wider audience. The entity registrar can be thought of as similar to a DNS registrar.

The `<mddri:RegistrationInfo>` container element, defined below, MUST appear within the `<md:Extensions>` element of `<md:EntityDescriptor>` or `<md:EntitiesDescriptor>` elements. The use of `<mddri:RegistrationInfo>`, or any other element defined in this section, outside of that context is not defined by this specification.

If the `<mddri:RegistrationInfo>` element appears in the `<md:Extensions>` element of a `<md:EntitiesDescriptor>`, then it applies to all descendant `<md:EntitiesDescriptor>` and `<md:EntityDescriptor>` elements.

The `<mddri:RegistrationInfo>` element MUST NOT appear more than once within the `<md:Extensions>` element of a given `<md:EntityDescriptor>` element.

2.2.1 Element `<mddri:RegistrationInfo>`

The `<mddri:RegistrationInfo>` contains information that describes the registrar of the entity represented by the contain `<md:EntityDescriptor>`.

`registrationAuthority` [Required]

The authority that registered the entity.
registrationInstant [Optional]

   The instant the entity was registered with the authority. This attribute SHOULD be populated for
   all newly registered entities but is optional because the registration instant may not have been
   tracked, by the registrar, for existing entities.

   Time values MUST be expressed in the UTC timezone using the 'Z' timezone identifier.

<mddri:RegistrationPolicy> [Optional]

   The policy under which the entity was registered.

   There SHOULD NOT be more than one <mddri:RegistrationPolicy>, within a given
   <mddri:DocumentInfo>, for a given language.

<element name="RegistrationInfo" type="mddri:RegistrationInfoType" />
<complexType name="RegistrationInfoType">
<sequence>
   <element ref="mddri:RegistrationPolicy" />
   <any namespace="#other" processContents="lax"/>
</sequence>
<attribute name="registrationAuthority" type="anyURI" use="required"/>
<attribute name="registrationInstant" type="dateTime"/>
<anyAttribute namespace="#other" processContents="lax"/>
</complexType>

2.2.2 Element <mddri:RegistrationPolicy>

   The <mddri:RegistrationPolicy> element is a URL to a localized description of the registration
   policy of the registrar. The URL MUST represent a single, immutable, policy document. Any changes
   made to an existing policy document MUST result in a new URL. The URL SHOULD resolve to a human
   readable form of the policy document for the entire period in which the policy may be in use.

<element name="RegistrationPolicy" type="md:localizedURIType"/>

2.3 Example

<EntitiesDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:mddri="urn:oasis:names:tc:SAML:metadata:dri">
<Extensions>
   <mddri:DocumentInfo creationInstant="2010-11-17T16:59:02Z">
      <mddri:UsagePolicy xml:lang="en">
      </mddri:UsagePolicy>
      <mddri:UsagePolicy xml:lang="de">
         http://www.switch.ch/aai/metadata/de_usage.html
      </mddri:UsagePolicy>
   </mddri:DocumentInfo>
</Extensions>

<EntityDescriptor entityID="https://aai-logon.switch.ch/idp/shibboleth">
<Extensions>
   <mddri:RegistrationInfo
      registrationAuthority="urn:mace:switch.ch:SWITCHaai"
      registrationInstant="2006-05-29T11:34:27Z">
      <mddri:RegistrationPolicy xml:lang="en">
         http://www.switch.ch/aai/metadata/en_registration.html
      </mddri:RegistrationPolicy>
      <mddri:RegistrationPolicy xml:lang="de">
      </mddri:RegistrationPolicy>
</mddri:RegistrationInfo>
</Extensions>

<saml-metadata-dri-v1.0-wd01>
Working Draft
Copyright © OASIS® 2010. All Rights Reserved.
Standards Track Work Product
Page 8 of 12
24 November 2010
<IDPSSODescriptor
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <SingleSignOnService
    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    Location="https://aai-logon.switch.ch/idp/profile/SAML2/POST/SSO"/>
</IDPSSODescriptor>

</EntityDescriptor>

<EntityDescriptor entityID="urn:mace:incommon:osu.edu">
  <Extensions>
    <mddri:DocumentInfo>
      <mddri:PublicationPath>
        <mddri:Publication publisher="urn:mace:incommon" serialNumber="ABC123"/>
      </mddri:PublicationPath>
    </mddri:DocumentInfo>
    <mddri:RegistrationInfo
      registrationAuthority="urn:mace:incommon">
      <mddri:RegistrationPolicy xml:lang="en">
        http://www.incommonfederation.org/metadata/en_registration.html
      </mddri:RegistrationPolicy>
    </mddri:RegistrationInfo>
  </Extensions>

  <IDPSSODescriptor
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol">
    <SingleSignOnService
      Binding="urn:mace:shibboleth:1.0:profiles:AuthnRequest"
      Location="https://idp.ohio-state.edu/idp/profile/Shibboleth/SSO"/>
  </IDPSSODescriptor>
</EntityDescriptor>
</EntitiesDescriptor>
3 Conformance

3.1 SAML V2.0 Metadata Extensions for Documentation and Registration Information Version 1.0

A metadata producer conforms to this profile if it has the ability to produce metadata in accordance with sections 2.1 and 2.2.
Appendix A. Acknowledgments

The editors would like to acknowledge the contributions of the OASIS Security Services Technical Committee, whose voting members at the time of publication were:

- TBD

The editor would also like to acknowledge the following contributors:

- Scott Cantor, The Ohio State University
- Ian Young, EDINA, University of Edinburgh
Appendix B. Revision History