SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0

Working Draft 01
6 September 2010

Specification URIs:

This Version:
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui-cd-01.html
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui-cd-01.odt (Authoritative)

Previous Version:
None

Latest Version:
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui.html
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui.odt (Authoritative)
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui.pdf

Technical Committee:
OASIS Security Services TC

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

Editor(s):
Scott Cantor, Internet2

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

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

Abstract:
This document defines a set of extensions to SAML metadata that provide information necessary for user agents to present effective user interfaces and, in the case of identity provider discovery, recommend appropriate choices to the user.

Status:
This document was last revised or approved by the SSTC on the above date. The level of approval is also listed above. Check the current location noted above for possible later revisions of this document. This document is updated periodically on no particular schedule.
TC members should send comments on this specification to the TC’s email list. Others should send comments to the TC by using the “Send A Comment” button on the TC’s web page at [http://www.oasis-open.org/committees/security](http://www.oasis-open.org/committees/security).

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the IPR section of the TC web page ([http://www.oasis-open.org/committees/security/ipr.php](http://www.oasis-open.org/committees/security/ipr.php)).

The non-normative errata page for this specification is located at [http://www.oasis-open.org/committees/security](http://www.oasis-open.org/committees/security).
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 Notation</td>
<td>5</td>
</tr>
<tr>
<td>1.2 Normative References</td>
<td>5</td>
</tr>
<tr>
<td>2 Metadata Extensions for Login and Discovery User Interface</td>
<td>7</td>
</tr>
<tr>
<td>2.1 User Interface Information</td>
<td>7</td>
</tr>
<tr>
<td>2.1.1 Element <a href="">md:UIInfo</a></td>
<td>7</td>
</tr>
<tr>
<td>2.1.2 Element <a href="">mdui:DisplayName</a></td>
<td>8</td>
</tr>
<tr>
<td>2.1.3 Element <a href="">mdui:Description</a></td>
<td>8</td>
</tr>
<tr>
<td>2.1.4 Element <a href="">mdui:Logo</a></td>
<td>8</td>
</tr>
<tr>
<td>2.1.5 Element <a href="">mdui:InformationURL</a></td>
<td>9</td>
</tr>
<tr>
<td>2.1.6 Element <a href="">mdui:PrivacyStatementURL</a></td>
<td>9</td>
</tr>
<tr>
<td>2.2 Discovery Hinting Information</td>
<td>9</td>
</tr>
<tr>
<td>2.2.1 Element <a href="">mdui:DiscoHints</a></td>
<td>9</td>
</tr>
<tr>
<td>2.2.2 Element <a href="">mdui:PHint</a></td>
<td>10</td>
</tr>
<tr>
<td>2.2.3 Element <a href="">mdui:DomainHint</a></td>
<td>10</td>
</tr>
<tr>
<td>2.2.4 Element <a href="">mdui:GeolocationHint</a></td>
<td>10</td>
</tr>
<tr>
<td>2.3 Relationship with Existing Metadata Elements</td>
<td>10</td>
</tr>
<tr>
<td>2.3.1 <a href="">md:Organization</a> Elements</td>
<td>10</td>
</tr>
<tr>
<td>2.3.2 Service Name and Description</td>
<td>11</td>
</tr>
<tr>
<td>2.3.3 Suggested Precedence</td>
<td>11</td>
</tr>
<tr>
<td>2.4 Example</td>
<td>11</td>
</tr>
<tr>
<td>3 Conformance</td>
<td>13</td>
</tr>
<tr>
<td>3.1 SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0</td>
<td>13</td>
</tr>
</tbody>
</table>
1 Introduction

SAMLV2.0 metadata [SAML2Meta] provides a mechanism for expressing information necessary for SAML entities to successfully communicate with each other. However in most SAML profiles there is also a user agent involved, usually representing an actual person, that also participates in the profiled message exchanges. This document defines a set of extensions to metadata that provide information necessary for user agents to present effective user interfaces and, in the case of identity provider discovery, provide for recommendation of appropriate choices to the user.

There are existing, though incomplete, metadata elements that carry some of this information, but existing practice around their use is inconsistent, and defining extensions with more well-defined semantics is less disruptive to existing metadata deployments.

1.1 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 [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.

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>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>mdui:</td>
<td>urn:oasis:names:tc:SAML:2.0:metadata:ui</td>
<td>This is the SAML V2.0 metadata extension namespace defined by this document and its accompanying schema [MetaUI-XSD].</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>
</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 Login and Discovery User Interface

2.1 User Interface Information

The user interface extension elements are oriented towards the requirements of user agent presentation of entities represented by SAML metadata, typically as part of identity provider discovery or representing services requesting information from a user’s identity provider.

The \(<\texttt{md:UIInfo}\>\) container element, defined below, MUST appear within the \(<\texttt{md:Extensions}\>\) element of a role element (one whose type is based on \texttt{md:RoleDescriptorType}). The use of the \(<\texttt{md:UIInfo}\>\) element, or any other element defined in this section, outside of that context is not defined by this specification.

2.1.1 Element \(<\texttt{md:UIInfo}\>\)

The \(<\texttt{md:UIInfo}\>\) element contains information which pertains to (but is not specifically limited to) the creation of user interfaces for tasks such as identity provider selection/discovery, user authentication, attribute release consent, etc.

This element contains any number of the following elements, in any order:

\(<\texttt{md:DisplayName}\>\)
Localized names for the entity operating in the containing role.

\(<\texttt{md:Description}\>\)
Localized descriptions of the entity operating in the containing role.

\(<\texttt{md:Logo}\>\)
Localized logo graphic for the entity operating in the containing role.

\(<\texttt{md:InformationURL}\>\)
URLs to localized information about the entity operating in the containing role.

\(<\texttt{md:PrivacyStatementURL}\>\)
URLs to localized information about the privacy practices of the entity operating in the containing role.

In addition, this element MAY contain an arbitrary number of extension elements from other namespaces, the definitions/semantics of which must be supplied elsewhere.

The schema for the \(<\texttt{md:UIInfo}\>\) element, and its corresponding \texttt{mdui:UIInfoType} complex type, is as follows:

```xml
<element name="UIInfo" type="mdui:UIInfoType"/>
<complexType name="UIInfoType">
  <choice minOccurs="0" maxOccurs="unbounded">
    <element ref="mdui:DisplayName"/>
    <element ref="mdui:Description"/>
    <element ref="mdui:Logo"/>
    <element ref="mdui:InformationURL"/>
    <element ref="mdui:PrivacyStatementURL"/>
    <any namespace="##other" processContents="lax"/>
  </choice>
</complexType>
```
2.1.2 Element <mdui:DisplayName>

The <mdui:DisplayName> element specifies a set of localized names fit for display to users. Such names are meant to allow a user to distinguish and identify the entity acting in a particular role.

There MUST NOT be more than one <mdui:DisplayName> element with the same xml:lang attribute value within a single role descriptor.

The schema for the <mdui:DisplayName> element is as follows:

```
<element name="DisplayName" type="md:localizedNameType"/>
```

2.1.3 Element <mdui:Description>

The <mdui:Description> element specifies a brief, localized description fit for display to users. In the case of an <md:SPSSODescriptor> role, this SHOULD be a description of the service being offered. In the case of an <md:IDPSSODescriptor> role this SHOULD be a description of the user community serviced.

In all cases this text MUST be standalone, meaning it is not to be used as a template requiring additional text (e.g., "This service offers $description").

There MUST NOT be more than one <mdui:Description> element with the same xml:lang attribute value within a single role descriptor.

The schema for the <mdui:Description> element is as follows:

```
<element name="Description" type="md:localizedNameType"/>
```

2.1.4 Element <mdui:Logo>

The <mdui:Logo> element specifies the external location of a localized logo fit for display to users. This element extends the anyURI schema type with the following attributes:

- **height** [Required]
  - The height of the logo measured in pixels.

- **width** [Required]
  - The width of the logo measured in pixels.

- **xml:lang**
  - Optional language specifier.

If a logo without an xml:lang attribute is present, then it SHOULD be considered the default logo for use when a logo in the user's preferred language is not available.

In order to facilitate the usage of logos within a user interface, logos SHOULD:

- use a transparent background where appropriate
- use PNG, or GIF (less preferred), images
- use HTTPS URLs in order to avoid mixed-content warnings within browsers

Entities SHOULD offer at least one logo that measures 16 x 16 in pixels, and at least one logo with a 16:9 aspect ratio.

The schema for the <mdui:Logo> element, and its corresponding mdui:LogoType complex type, is as follows:

```
<element name="Logo" type="mdui:LogoType"/>
<complexType name="LogoType">
  <simpleContent>
    <extension base="anyURI">
```

15  draft-sstc-saml-metadata-ui-01
16  Copyright © OASIS® 2010. All Rights Reserved.
2.1.5 Element <mdui:InformationURL>

The <mdui:InformationURL> specifies an external location for localized information about the entity acting in a given role meant to be viewed by users. The content found at the URL SHOULD provide more complete information than what would be provided by the <mdui:Description> element.

There MUST NOT be more than one <mdui:InformationURL> element with the same xml:lang attribute value within a single role descriptor.

The schema for the <mdui:InformationURL> element is as follows:

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

2.1.6 Element <mdui:PrivacyStatementURL>

The <mdui:PrivacyStatementURL> specifies an external location for localized privacy statements. Such statements are meant to provide a user with information about how information will be used and managed by the entity acting in a given role.

There MUST NOT be more than one <mdui:PrivacyStatementURL> element with the same xml:lang attribute value within a single role descriptor.

The schema for the <mdui:PrivacyStatementURL> element is as follows:

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

2.2 Discovery Hinting Information

The discovery hinting extension elements provide information which may hint at the identity provider with which a user is associated.

The <mdui:DiscoHints> container element, defined below, MUST appear within the <md:Extensions> element of an <md:IDPSSODescriptor> element. The use of the <mdui:DiscoHints> element, or any other element defined in this section, outside of that context is not defined by this specification.

Information provided by the content of this element is meant only as a hint and SHOULD NOT be used to definitively select an identity provider without user intervention or confirmation.

2.2.1 Element <mdui:DiscoHints>

The <mdui:DiscoHints> element contains information which may be used by an identity provider selection/discovery service as hints in determining with which identity provider(s) the user may be associated.

This element contains any number of the following elements, in any order:

- <mdui:IPHint>
  - IP address blocks associated with, or serviced by, the entity operating in the containing role.
In addition, this element MAY contain an arbitrary number of extension elements from other namespaces, the definitions/semantics of which must be supplied elsewhere.

The schema for the `<mdui:DiscoHints>` element, and its corresponding `mdui:DiscoHintsType` complex type, is as follows:

```
<element name="DiscoHints" type="mdui:DiscoHintsType"/>
<complexType name="DiscoHintsType">
  <choice minOccurs="0" maxOccurs="unbounded">
    <element ref="mdui:IPHint"/>
    <element ref="mdui:DomainHint"/>
    <element ref="mdui:GeolocationHint"/>
  </choice>
</complexType>
```

### 2.2.2 Element `<mdui:IPHint>`

The `<mdui:IPHint>` element specifies an [RFC4632] block associated with, or serviced by, the entity. Both IPv4 and IPv6 CIDR blocks MUST be supported.

The schema for the `<mdui:IPHint>` element is as follows:

```
<element name="IPHint" type="string"/>
```

### 2.2.3 Element `<mdui:DomainHint>`

The `<mdui:DomainHint>` element specifies a DNS domain associated with, or serviced by, the entity.

The schema for the `<mdui:DomainHint>` element is as follows:

```
<element name="DomainHint" type="string"/>
```

### 2.2.4 Element `<mdui:GeolocationHint>`

The `<mdui:GeolocationHint>` element specifies a set of geographic coordinates associated with, or serviced by, the entity. Coordinates are given in URI form using the `geo` URI scheme [RFC5870].

The schema for the `<mdui:GeolocationHint>` element is as follows:

```
<element name="GeolocationHint" type="anyURI"/>
```

### 2.3 Relationship with Existing Metadata Elements

#### 2.3.1 `<md:Organization>` Elements

SAML metadata defines localized organizational names, display names, and URLs at both the entity and role level. These elements are meant to reflect information about the organization that “owns” or operates a particular entity. To date, most known identity provider discovery interfaces have relied on entity-level `<md:OrganizationDisplayName>` element content. Some applications will also display the organization name for service providers as a means of identifying the service.

However, such usage is based on two implicit assumptions:
• the organization name is recognizable and can be understood by the user within the context that it is used
• the organization only has one entity operating in a given role at any specific time

There are many cases, however, where one or both of these assumption are not true. An example conflicting with the first assumption may be Virginia Polytechnic Institute and State University, which the world knows as "Virginia Tech". An example that conflicts with both assumptions might be a third-party hosting service. Its name would not be recognized by any user and it could operate many entities at any given time.

However, the organizational display name may still be useful, for example within "owned by..." or "operated by..." statements.

2.3.2 Service Name and Description

Entities with a <md:SPSSODescriptor> role may optionally include one or more <md:AttributeConsumingService> elements which in turn contain <md:ServiceName> and <md:ServiceDescription> elements. These elements are normally used to expose the attribute requirements for various service "levels" and to associate certain names and descriptions with them.

The following issues make these elements inappropriate for carrying a general display name and description for the service:

• other role elements have no analogous elements
• some services do not require attributes, but the <md:AttributeConsumingService> element requires the inclusion of one or more <md:RequestedAttribute> elements
• the typical usage for these elements do not convey a name and description for the service itself

2.3.3 Suggested Precedence

Implementations that rely on display name information SHOULD rely on elements in the following order of preference:

• <mdui:DisplayName>
• <md:ServiceName> (if applicable)
• <md:OrganizationDisplayName>
• entityID

2.4 Example

An elided example follows.

```xml
<EntityDescriptor entityID="https://idp.switch.ch/idp/shibboleth"
    xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:mdui="urn:oasis:names:tc:SAML:2.0:metadata:ui">
    <IDPSSODescriptor
        protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <Extensions>
            <mdui:UIInfo>
                <mdui:DisplayName xml:lang="en">SWITCH</mdui:DisplayName>
            </mdui:UIInfo>
        </Extensions>
    </IDPSSODescriptor>
</EntityDescriptor>
```
<mdui:DisplayName xml:lang="de">SWITCH</mdui:DisplayName>

<mdui:Description xml:lang="en">
  Switzerland's national research and education network.
</mdui:Description>

<mdui:Description xml:lang="de">
  Das schweizerische Hochschul- und Forschungsnetzwerk.
</mdui:Description>

<mdui:Logo href="http://switch.ch" height="51" width="172">
  http://switch.ch/resources/images/logo.gif
</mdui:Logo>

<mdui:InformationURL xml:lang="en">
  http://switch.ch
</mdui:InformationURL>

<mdui:InformationURL xml:lang="de">
  http://switch.ch/de
</mdui:InformationURL>

</mdui:UIInfo>

<mdui:DiscoHints>
  <mdui:IPHint>130.59.0.0/16</mdui:IPHint>
  <mdui:IPHint>2001:620::0/96</mdui:IPHint>
  <mdui:DomainHint>switch.ch</mdui:DomainHint>
  <mdui:GeolocationHint>geo:47.37328,8.531126</mdui:GeolocationHint>
</mdui:DiscoHints>

<!-- other role-level elements -->

</IDPSSODescriptor>

</EntityDescriptor>
3 Conformance

3.1 SAML V2.0 Metadata Extensions for Login and Discovery User Interface 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.

A metadata consumer conforms to this profile if it can consume extended metadata produced in accordance with sections 2.1 and 2.2.

An identity provider discovery service or agent conforms to this profile if it has the ability to consume and utilize extended metadata produced in accordance with sections 2.1, 2.2, and 2.3.3.
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:

- Chad LaJoie, Itumi, LLC.
- Rod Widdowson, Steading Software
- Ian Young, EDINA, University of Edinburgh
Appendix B. Revision History

Working Draft 01

- Initial OASIS submission
- Removed SAML version number from namespace for consistency with other extensions
- Various editorial rewording and combining of normative sections, externalized the schema.
- Added conformance section
- Changed base type of <Logo> to URI, and switched <GeolocationHint> to URI based on RFC5870.
- Added wildcards to wrapper elements, changed them to choice bags.

Presubmission Changes:

Changes to Draft 03:

- Correct typo in DiscoHints schema; the ‘s’ was missing from Hints
- Add a couple examples where the assumptions noted in section 2.3.1 do not hold
- Minor typographical corrections

Changes to Draft 02:

- Add SAML version number to declared namespace
- Add <UIInfo> and <DiscoHints>

Changes to Draft 01:

- Move from the use of metadata entity attributes to direct XML elements located with in role <Extensions> elements
- Make xml:lang attribute on <Logo> elements optional with the lack of language indicating the default logo to use
- Add <PrivacyStatementURL> element