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

Candidate OASIS Standard 01

11 July 2019

This version:
https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/cos01/sstc-saml-metadata-ui-v1.0-cos01.odt (Authoritative)
https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/cos01/sstc-saml-metadata-ui-v1.0-cos01.html
https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/cos01/sstc-saml-metadata-ui-v1.0-cos01.pdf

Previous version:
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/cs01/sstc-saml-metadata-ui-v1.0-cs01.odt (Authoritative)
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/cs01/sstc-saml-metadata-ui-v1.0-cs01.html
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/cs01/sstc-saml-metadata-ui-v1.0-cs01.pdf

Latest version:
https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/sstc-saml-metadata-ui-v1.0.odt (Authoritative)
https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/sstc-saml-metadata-ui-v1.0.html
https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/sstc-saml-metadata-ui-v1.0.pdf

Technical Committee:
OASIS Security Services (SAML) TC

Chair:
Thomas Hardjono (hardjono@mit.edu), M.I.T.

Editor:
Scott Cantor (cantor.2@osu.edu), Internet2

Additional artifacts:
This prose specification is one component of a Work Product that also includes:

- XML schema: https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/cos01/xsd/

Related work:
This specification defines extensions for use with:

- *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0*. March 2005. OASIS Standard. http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf

Declared XML namespaces:

- 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 OASIS Security Services (SAML) TC on the above date. The level of approval is also listed above. Check the "Latest version" location noted above for possible later revisions of this document. Any other numbered Versions and other technical work produced by the Technical Committee (TC) are listed at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security#technical.

TC members should send comments on this document to the TC's email list. Others should send comments to the TC's public comment list, after subscribing to it by following the instructions at the "Send A Comment" button on the TC's web page at https://www.oasis-open.org/committees/security/.

This specification is provided under the RF on RAND Terms Mode of the OASIS IPR Policy, the mode chosen when the Technical Committee was established. 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 Intellectual Property Rights section of the TC's web page (https://www.oasis-open.org/committees/security/ipr.php).

Note that any machine-readable content (Computer Language Definitions) declared Normative for this Work Product is provided in separate plain text files. In the event of a discrepancy between any such plain text file and display content in the Work Product's prose narrative document(s), the content in the separate plain text file prevails.

Citation format:

When referencing this specification the following citation format should be used:

[SAML-Metadata-UI-V1.0]
SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0. Edited by Scott Cantor. 11 July 2019. Candidate OASIS Standard 01. https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/cos01/sstc-saml-metadata-ui-v1.0-cos01.html. Latest version: https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/sstc-saml-metadata-ui-v1.0.html.

Notices

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, and 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.

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 OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

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' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on 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 OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The name "OASIS" is a trademark of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see https://www.oasis-open.org/policies-guidelines/trademark for above guidance.

Table of Contents

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 IPR Policy

This specification is provided under the RF on RAND Terms Mode of the OASIS IPR Policy, the mode chosen when the Technical Committee was established. 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 Intellectual Property Rights section of the TC's web page (https://www.oasis-open.org/committees/security/ipr.php).

1.2 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. 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:

Prefix	XML Namespace	Comments
`md:`	urn:oasis:names:tc:SAML:2.0:metadata	This is the SAML V2.0 metadata namespace defined in the SAML V2.0 metadata specification **[SAML2Meta]** .
`mdui:`	urn:oasis:names:tc:SAML:metadata:ui	This is the SAML V2.0 metadata extension namespace defined by this document and its accompanying schema.
`xsd:`	http://www.w3.org/2001/XMLSchema	This namespace is defined in the W3C XML Schema specification **[Schema1]** . In schema listings, this is the default namespace and no prefix is shown.

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.
```

1.3 Normative 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

[RFC4632] V. Fuller et al. Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan. IETF RFC 4632, August 2006. http://www.ietf.org/rfc/rfc4632.txt

[RFC5870] A. Mayrhofer et al. A Uniform Resource Identifier for Geographic Locations ('geo' URI). IETF RFC 5870, June 2010. http://www.ietf.org/rfc/rfc5870.txt

[SAML2Errata] SAML V2.0 Errata. 1 December 2009. OASIS Approved Errata. http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.pdf

[SAML2Meta] Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0. 15 March 2005. OASIS Standard. http://docs.oasis-open.org/security/saml/v2.0/saml- metadata-2.0-os.pdf

[Schema1] H. S. Thompson et al. XML Schema Part 1: Structures. World Wide Web Consortium Recommendation, May 2001. http://www.w3.org/TR/2001/REC- xmlschema-1-20010502/

[Schema2] Paul V. Biron, Ashok Malhotra. XML Schema Part 2: Datatypes. World Wide Web Consortium Recommendation, May 2001. http://www.w3.org/TR/2001/REC- xmlschema-2-20010502/

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 specifics of such presentation and the use of the elements that follow is not in scope for this specification, but communities of use SHOULD establish guidelines and even prescriptive requirements to encourage consistency and understandability for users.

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

This element, if it appears, MUST contain at least one child element.

Finally, this element MUST NOT appear more than once within a given `<md:Extensions>` element.

2.1.1 Element <mdui:UIInfo>

The `<mdui: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:

`<mdui:DisplayName>`

A localized name for the entity operating in the containing role.

`<mdui:Description>`

A localized description of the entity operating in the containing role.

`<mdui:Keywords>`

Localized search keywords, tags, categories, or labels for the containing role.

`<mdui:Logo>`

A localized logo image for the entity operating in the containing role.

`<mdui:InformationURL>`

A URL to localized information about the entity operating in the containing role.

`<mdui:PrivacyStatementURL>`

A URL 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 `<mdui:UIInfo>` element, and its corresponding **mdui:UIInfoType** complex type, is as follows:

```
<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:Keywords"/>
      <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 localized name fit for display to users. Such names are meant to allow a user to distinguish and identify the entity acting in a particular role. The content of this element should be suitable for use in constructing accessible user interfaces for those with disabilities.

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 include 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:Keywords>

The `<mdui:Keywords>` element specifies a list of localized search keywords, tags, categories, or labels that apply to the containing role. This element extends the **mdui:listOfStrings** schema type with the following attribute:

`xml:lang` [Required]

Language specifier.

The content of this element is a "list" of strings in the XML Schema **[Schema2]** sense, which means the keyword strings are space-delimited. Spaces within individual keywords are encoded with a “plus” (+) character; as a consequence, keywords may not contain that character.

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

The schema for the `<mdui:Keywords>` element, and its corresponding **mdui:KeywordsType** complex type, is as follows:

```
<element name="Keywords" type="mdui:KeywordsType"/>
<complexType name="KeywordsType">
   <simpleContent>
      <extension base="mdui:listOfStrings">
         <attribute ref="xml:lang" use="required"/>
      </extension>
   </simpleContent>
</complexType>
<simpleType name="listOfStrings">
```

```
   <list itemType="string"/>
</simpleType>
```

2.1.5 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 rendered height of the logo measured in pixels.

`width` [Required]

The rendered width of the logo measured in pixels.

`xml:lang`

Optional language specifier.

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

The order of logo elements is not significant, and a consumer MAY select any logo that meets its presentation and internationalization requirements. Communities of use SHOULD establish guidelines or requirements for logo size, aspect ratio, etc. to ensure consistency. If logos without an `xml:lang` attribute are present, then they SHOULD be considered the default logos for use when logos in the user's preferred language are not available.

Note that while vector graphic formats may be renderable at many sizes, the `height` and `width` attributes remain mandatory to allow consumers that lack intelligence regarding image processing to locate images suitable for particular sizes. The same image MAY be specified with multiple sizes when appropriate.

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">
         <attribute name="height" type="positiveInteger" use="required"/>
         <attribute name="width" type="positiveInteger" use="required"/>
         <attribute ref="xml:lang"/>
      </extension>
   </simpleContent>
</complexType>
```

2.1.6 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:

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

2.1.7 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:

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

2.2 Discovery Hinting Information

The discovery hinting extension elements provide information that hints at the identity provider with which a user is associated. A server-side selection mechanism could leverage such hints in conjunction with client-supplied information to adjust likely choices.

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. As a consequence, hints are inappropriate to use in conjunction with discovery protocols or protocol features that would prevent user interaction.

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.

This element, if it appears, MUST contain at least one child element.

Finally, this element MUST NOT appear more than once within a given <md:Extensions> element.

2.2.1 Element <mdui:DiscoHints>

The <mdui:DiscoHints> element contains information that 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.

<mdui:DomainHint>

DNS domain names associated with, or serviced by, the entity operating in the containing role.

<mdui:GeolocationHint>

Geographic coordinates 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"/>
      <any namespace="##other" processContents="lax"/>
   </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 Security Considerations

The information contained in these extensions, as well as the content identified by various URLs, is intended for the construction of user interfaces. As such, special consideration by implementers and deployers is warranted.

Any URLs MUST be carefully sanitized and encoded to protect against cross-site scripting and related vulnerabilities. Schemes other than “https”, “http”, or “data” SHOULD NOT be used.

Since it is generally impractical to guarantee the continued safety of content behind a particular URL, the use of “https” URLs is RECOMMENDED, and control over the URLs in question must be carefully established by the publisher of metadata containing these extensions. Consumers of metadata using these extensions to construct UIs must ensure the provenance of metadata and that the processes by which the extensions are managed by the publisher are sufficiently sound.

This is particularly relevant for the `<mdui:Logo>` element, since such URLs are often dereferenced by the user agent without intervention. Where practical, the use of server-side image processing may enable a higher degree of safety and control over the presentation of images than direct embedding of links to logos.

2.4 Relationship with Existing Metadata Elements

2.4.1 <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.

2.4.2 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
- one typical usage for these elements may not convey a name and description for the service itself, but rather for some aspect of the service (e.g., a service level, or a type of access)

2.4.3 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)
- `entityID` or a hostname associated with the endpoint of the service

As a consequence, entities may rely on the existing `<md:ServiceName>` (or where appropriate the `<md:ServiceDescription>`) element by omitting the `<mdui:DisplayName>` (or `<mdui:Description>`) element from their metadata.

Note that when multiple `<md:AttributeConsumingService>` elements are used, some identity or discovery protocols may lack the ability to signal which of the multiple elements is relevant to a request. In such deployments, limiting the cardinality to a single element or requiring the use of the `<mdui:DisplayName>` element may be necessary.

Implementations MAY support the use of `<md:OrganizationDisplayName>`, particularly as a migration strategy, but this is not recommend this as a general practice.

2.5 Example

An elided example follows.

```
<EntityDescriptor entityID="https://idp.switch.ch/idp/shibboleth"
                  xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
                  xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui">

  <IDPSSODescriptor
      protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <Extensions>
```

```
      <mdui:UIInfo>

         <mdui:DisplayName xml:lang="en">SWITCH</mdui:DisplayName>
         <mdui:DisplayName xml:lang="de">SWITCH</mdui:DisplayName>

         <mdui:Description xml:lang="en">
            Switzerland's national research and eduction network.
         </mdui:Description>
         <mdui:Description xml:lang="de">
            Das schweizerische Hochschul- und Forschungsnetzwerk.
         </mdui:Description>

         <mdui:Logo height="16" width="16">
             https://switch.ch/resources/images/smalllogo.png
         </mdui:Logo>
         <mdui:Logo height="97" width="172">
             https://switch.ch/resources/images/logo.png
         </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>
    </Extensions>

    <!-- 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 2.4.3.

Appendix A Acknowledgments

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

- Scott Cantor, Internet2
- Nate Klingenstein, Internet2
- Chad LaJoie, Internet2
- Thomas Hardjono, M.I.T.
- Thinh Nguyenphu, Nokia Siemens Networks GmbH
- Hal Lockhart, Oracle
- Anil Saldhana, Red Hat

The editor would also like to acknowledge the following contributors:

- Rod Widdowson, EDINA, University of Edinburgh
- Ian Young, EDINA, University of Edinburgh

Appendix B Revision History

Working Draft 10:

- Address public comments from http://wiki.oasis-open.org/security/PublicComments20111014-20111113

Working Draft 09:

- Clarify lack of support for '+' in keywords
- s/then/than

Working Draft 08:

- Fix namespace in example

Working Draft 07:

- Remove normative reference to schema (can't be kept current with document process)
- Allow for spaces in keywords using '+' escape
- Add security considerations section
- Add TC member list

Working Draft 06:

- Add `<Keywords>` element as a search "catch-all"

Working Draft 05:

- Fix typo
- Reword "languageless logo" text and move together with other logo use guideline text

Working Draft 04:

- Migrated text to new OASIS template and filename
- Removed specific logo guidance in favor of generic advice
- Added fallback option to hostnames in addition to entityID
- Better guidance on intended use of elements and scope of specification

Working Draft 03:

- Fixed namespace in section 1 table
- Add limit on one wrapper element per Extensions block
- Improve example to reflect guidance in spec
- Add note about accessibility to DisplayName

Working Draft 02:

- Fixed missing wildcard in schema
- Corrected some typos
- Removed ODN from fallback precedence

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