# Identity Provider Discovery Service Protocol

## Draft 01, 30 January, 2007

**Document identifier:**

draft-sstc-saml-idp-discovery-01

**Location:**

http://www.oasis-open.org/committees/documents.php?wg_abbrev=security

**Technical Committee:**

OASIS Security Services TC

**Chair(s):**

Hal Lockhart, BEA Systems, Inc.

Prateek Mishra, Oracle Corporation

**Editor(s):**

Rod Widdowson, Edinburgh University

Scott Cantor, Internet2

**Related Work:**

This specification is an alternative to the SAML V2.0 Identity Provider Discovery profile in the SAML V2.0 Profiles specification [SAML2Prof].

**Abstract:**

Defines a generic browser-based protocol by which a centralized discovery service can provide a requesting service provider with the unique identifier of an identity provider that can authenticate a principal.

**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.

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.

The non-normative errata page for this specification is located at http://www.oasis-open.org/committees/security.

# 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.

# Table of Contents

# 1 Introduction

This specification defines a browser-based protocol by which a centralized discovery service can provide a requesting service provider with the unique identifier of an identity provider that can authenticate a principal. Thus, the protocol provides an alternative means of addressing section 4.1.3.2 of [SAML2Prof]. The profile for discovery defined in section 4.3 of [SAML2Prof] is similar, but has different deployment properties, such as the requirement for a shared domain.

Instead, this profile relies on a normative redirect-based wire protocol that allows for indepdenent implementation and deployment of the service provider and discovery service components, a model that has proven interesting in some large-scale deployments in which managing common domain membership may be impractical.

Note that most Web SSO protocols and profiles, including the multiple versions of SAML, share similar properties and requirements for identity provider discovery (although terminology often differs). This protocol, while well-suited to SAML V2.0 SSO requirements, is not specific to them.

## 1.1 Terminology

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 [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.

```
Listings of XML 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:

| 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]. |
| idpdisc: | urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-protocol | This is the SAML V2.0 metadata extension namespace defined by this document and its accompanying schema [IDPDisco-XSD]. |
| 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: <SAMLElement>, <ns:ForeignElement>, Attribute, **Datatype**, OtherKeyword.

## 1.2 Normative References

**[RFC 2119]** S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF RFC 2119, March 1997. http://www.ietf.org/rfc/rfc2119.txt.

**[IDPDisco-XSD]** S. Cantor et al. Metadata Extension Schema for Identity Provider Discovery Service Protocol, OASIS SSTC January 2007. Document ID sstc-saml-idp-discovery.xsd. See http://www.oasis-open.org/committees/security/.

**[SAML2Core]** S. Cantor et al. Assertions *and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Standard, March 2005. Document ID saml-core-2.0-os. See http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf.

**[SAML2Meta]** S. Cantor et al. *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Standard, March 2005. Document ID saml-metadata-2.0-os. See http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf.

**[SAML2Meta-xsd]** S. Cantor et al. SAML V2.0 metadata schema. OASIS Standard, March 2005. Document ID saml-schema-metadata-2.0. See http://docs.oasis-open.org/security/saml/v2.0/saml-schema-metadata-2.0.xsd.

**[SAML2Prof]** S. Cantor et al. *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Standard, March 2005. Document ID saml-profiles-2.0-os. See http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf.

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

# 2 Identity Provider Discovery Service Protocol

## 2.1 Required Information

**Identification:** `urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-protocol`

**Contact information:** security-services-comment@lists.oasis-open.org

**Description:** Given below.

**Updates:** Provides an alternative to the cookie-based discovery profile in section 4.3 of [SAML2Prof].

## 2.2 Protocol Description

This protocol can be used during web-based SSO when a service provider needs to establish which identity provider is associated with a principal. It is assumed that the user wields a standard HTTP user agent.

The discovery protocol encompases three steps, covering two normative message exchanges:

### 2.2.1 HTTP request to discovery service

In the first step, a requesting service provider redirects the user agent to the discovery service with an HTTP GET request.

The following parameters MUST be present on the query string (and URL-encoded):

`entityID`

The unique identifier of the service provider the end user is (or will be) interacting with, following successful authentication by an identity provider.

`return`

A URL, which MAY itself include a query string. The discovery service MUST redirect the user agent to this location in response to this request (see section 2.2.3).

`returnIDParam`

A parameter name used to return the unique identifier of the selected identity provider to the original requester.

The following parameters MAY be present:

`isPassive`

A boolean value of "true" or "false" that controls whether the discovery service is allowed to visibly interact with the user agent in the second step below. If a value is not provided, the default is "false".

### 2.2.2 Discovery service determines appropriate identity provider

In this step, the discovery service and user agent interact via unspecified means in order to establish the user's choice of identity provider. This may involve user selection, hints obtained through various means, and filtering based on the service provider (identified by the `entityID` parameter in step 1 above), preferred SSO protocols or profiles, etc.

If the isPassive parameter is set to “true”, the discovery service MUST NOT visibly take control of the user interface from the requesting service provider and interact with the user agent in a noticeable fashion. Additional redirection is permitted, however, provided the passive guarantee can be met.

The discovery service MAY rely on saved state, such as a browser cookie, to determine the appropriate identity provider. If a cookie is used, it SHOULD conform to the name and format specified by the Identity Provider Discovery Profile in section 4.3 of [SAML2Prof].

### 2.2.3 HTTP request to service provider

In the final step, the discovery service redirects the user agent back to the requesting service provider with an HTTP GET request, at the location supplied in the return parameter in the original request in step 1.

If an identity provider has been determined, then its unique identifier MUST be included as the value of the parameter whose name was specified as the value of the returnIDParam parameter in the original request.

The discovery service MUST take care to preserve any query string that may already be present within the return URL.

## 2.3 Use of Metadata

All redirection-based SSO protocols share a common property in that the service provider is permitted to (and in most cases must) redirect the user agent to the identity provider. This creates opportunities for phishing-style attacks against the user's authentication credentials when weak (but extremely common) forms of authentication such as passwords are used.

This protocol has the potential for creating additional opportunities for phishing if arbitrary web sites are permitted to utilize the protocol and obtain the user's identity provider, the key piece of knowledge required to fake the expected authentication experience. To mitigate this threat, metadata can be used to limit the sites authorized to use a discovery service, without introducing heavier-weight security approaches such as message authentication.

A discovery service SHOULD require that the service providers making use of it supply metadata (out of band or using techniques such as those described in the SAML V2.0 Metadata specification [SAML2Meta]. An extension element, <idpdisc:DiscoveryResponse>, of type **md:EndpointType**, is used to define the acceptable locations to which the discovery service should respond with the user's identity provider.

Upon receiving a request, the discovery service SHOULD ensure that it recognizes the requesting service provider, as identified by the entityID parameter in the request. The location supplied in the return parameter SHOULD then be compared to the Location attribute of any <idpdisc:DiscoveryResponse> elements found in the <md:Extensions> element of the service provider's <md:SPSSODescriptor> element. (Note that the ResponseLocation endpoint attribute is unused in this profile.)

In the case that the return parameter includes a query string, the discovery service MAY ignore it for the purposes of this comparison.

The schema for the <idpdisc:DiscoveryResponse> element is as follows:

```
<schema
    targetNamespace="urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-
protocol"
    xmlns:idpdisc="urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-
protocol"
```

```
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns="http://www.w3.org/2001/XMLSchema"
    elementFormDefault="unqualified"
    attributeFormDefault="unqualified"
    blockDefault="substitution"
    version="1.0">
    <annotation>
        <documentation>
            Document identifier: sstc-saml-idp-discovery
            Location: http://www.oasis-
open.org/committees/documents.php?wg_abbrev=security
            Revision history:
            V1.0 (January 2007):
              Initial version.
        </documentation>
    </annotation>
    <import namespace="urn:oasis:names:tc:SAML:2.0:metadata"
        schemaLocation="saml-schema-metadata-2.0.xsd"/>
    <element name="DiscoveryResponse" type="md:EndpointType"/>
</schema>
```

# 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:

@@TODO for final publication

# Appendix B. Revision History

- Draft 01, initial draft based on document prepared by Rod for Shibboleth project