[MS-SPS2SAUTH]:
OAuth 2.0 Authentication Protocol: SharePoint Profile

Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation for protocols, file formats, languages, standards as well as overviews of the interaction among each of these technologies.
- **Copyrights.** This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you may make copies of it in order to develop implementations of the technologies described in the Open Specifications and may distribute portions of it in your implementations using these technologies or your documentation as necessary to properly document the implementation. You may also distribute in your implementation, with or without modification, any schema, IDL's, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.
- **Patents.** Microsoft has patents that may cover your implementations of the technologies described in the Open Specifications. Neither this notice nor Microsoft's delivery of the documentation grants any licenses under those or any other Microsoft patents. However, a given Open Specification may be covered by Microsoft Open Specification Promise or the Community Promise. If you would prefer a written license, or if the technologies described in the Open Specifications are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting iplg@microsoft.com.
- **Trademarks.** The names of companies and products contained in this documentation may be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights.
- **Fictitious Names.** The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

Reservation of Rights. All other rights are reserved, and this notice does not grant any rights other than specifically described above, whether by implication, estoppel, or otherwise.

Tools. The Open Specifications do not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments you are free to take advantage of them. Certain Open Specifications are intended for use in conjunction with publicly available standard specifications and network programming art, and assumes that the reader either is familiar with the aforementioned material or has immediate access to it.

Preliminary Documentation. This Open Specification provides documentation for past and current releases and/or for the pre-release (beta) version of this technology. This Open Specification is final documentation for past or current releases as specifically noted in the document, as applicable; it is preliminary documentation for the pre-release (beta) versions. Microsoft will release final documentation in connection with the commercial release of the updated or new version of this technology. As the documentation may change between this preliminary version and the final version of this technology, there are risks in relying on preliminary documentation. To the extent that you incur additional development obligations or any other costs as a result of relying on this preliminary documentation, you do so at your own risk.

Revision Summary

Date	Revision History	Revision Class	Comments
01/20/2012	0.1	New	Released new document.
04/11/2012	0.1	No change	No changes to the meaning, language, or formatting of the technical content.

Table of Contents

1 Introduction

The OAuth 2.0 Authentication Protocol – SharePoint Profile is used for the server to server authentication among the applications that communicate over REST. This profile specification describes the implementation of [MS-OAUTH2EX] OAuth 2.0 Authentication Protocol Extensions specification by an application (example: SharePoint Server) in order to authenticate itself with the other application services, like a mail server (example: Exchange Server) or a communication server (example: Lync Server).

The [MS-OAUTH2EX] OAuth 2.0 Authentication Protocol Extensions specification describes the parameters and protocol flow that extend the [IETFDRAFT-OAuth2.0] OAuth 2.0 Authentication Protocol and [IETFDRAFT-JWT] JSON Web Token specifications in order to enable the server to server (S2S) authentication capability over REST.

Sections 1.8, 2, and 3 of this specification are normative and can contain the terms MAY, SHOULD, MUST, MUST NOT, and SHOULD NOT as defined in RFC 2119. Sections 1.5 and 1.9 are also normative but cannot contain those terms. All other sections and examples in this specification are informative.

1.1 Glossary

MAY, SHOULD, MUST, SHOULD NOT, MUST NOT: These terms (in all caps) are used as described in [RFC2119]. All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT.

1.2 References

References to Microsoft Open Specifications documentation do not include a publishing year because links are to the latest version of the documents, which are updated frequently. References to other documents include a publishing year when one is available.

1.2.1 Normative References

We conduct frequent surveys of the normative references to assure their continued availability. If you have any issue with finding a normative reference, please contact dochelp@microsoft.com. We will assist you in finding the relevant information. Please check the archive site, http://msdn2.microsoft.com/en-us/library/E4BD6494-06AD-4aed-9823-445E921C9624, as an additional source.

[IETFDRAFT-JWT] Goland, Y., and Jones, M., "JSON Web Token (JWT) Specification Draft", 24 Sep 2010, http://www.ietf.org/mail-archive/web/oauth/current/msg04407.html

[IETFDRAFT-OAuth2.0] Hammer-Lahav, E., Ed., Recordon, D., and Hardt, D., "The OAuth 2.0 Authorization Protocol", draft-ietf-oauth-v2-22, http://tools.ietf.org/html/draft-ietf-oauth-v2-23

[MS-OAUTH2EX] Microsoft Corporation, "OAuth 2.0 Authentication Protocol Extensions".

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, http://www.rfc-editor.org/rfc/rfc2119.txt

[XMLNS] Bray, T., Hollander, D., Layman, A., et al., Eds., "Namespaces in XML 1.0 (Third Edition)", W3C Recommendation, December 2009, http://www.w3.org/TR/2009/REC-xml-names-20091208/

[XMLSCHEMA1] Thompson, H.S., Ed., Beech, D., Ed., Maloney, M., Ed., and Mendelsohn, N., Ed., "XML Schema Part 1: Structures", W3C Recommendation, May 2001, http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/

[XMLSCHEMA2] Biron, P.V., Ed. and Malhotra, A., Ed., "XML Schema Part 2: Datatypes", W3C Recommendation, May 2001, http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/

1.2.2 Informative References

None.

1.3 Overview

This document specifies the profile of server to server authentications performed by an application server with other services. For example, in a scenario where an application calls to a mail server the communication between those two services shall follow the specifications mentioned in this document.

Throughout this documentation the term application refers to the services, like SharePoint product, which offers functionalities that depend on collaboration among multiple services and hence require server to server authentication.

The S2S protocol itself is documented in the [MS-OAUTH2EX] OAuth 2.0 Authentication Protocol Extensions documentation.

Throughout this documentation for ease of read service principals are represented as simple strings and these are represented as PIDs (GUID values) in the wire.

Following table maps the simple strings to the PID values:

	Principal identifier (PID) value
microsoft.sharepoint	00000003-0000-0ff1-ce00-000000000000
microsoft.exchange	00000002-0000-0ff1-ce00-000000000000
microsoft.lync	00000004-0000-0ff1-ce00-000000000000
microsoft.sts	00000001-0000-0000-c000-000000000000

1.4 Relationship to Other Protocols

Other than the normative references made in this document, there are no other protocols that relate to this protocol.

1.5 Prerequisites/Preconditions

To make a request for S2S token the caller must reside in the same system as STS.

The caller must be running under the application pool account sharepoint\system. Note that this the default service application pool identity created in a typical SharePoint deployment.

1.6 Applicability Statement

This profile is applicable only when a service call is made through REST and to or from an application that supports server to server authentication.

Use this profile when calling to an application, which adheres to this SharePoint Profile, over REST.

Do not use this profile for non-REST-based calls, even if the application that is being called adheres to this profile.

1.7 Versioning and Capability Negotiation

None.

1.8 Vendor-Extensible Fields

None.

1.9 Standards Assignments

None.

2 Messages

2.1 Transport

The messages are transported over TCP and no specific parameters are passed to the transport.

This profile uses the transport for securing the tokens being sent on the wire i.e. it uses HTTPS.

This profile is not encoded by Open-Data [MS-DATA] and it uses the default character set defined by the client or the server.

Refer to Security in section 5 of this document for details.

2.2 Message Syntax

This section contains common definitions used by this protocol. The syntax of the definitions uses XML schema as defined in [XMLSCHEMA1] and [XMLSCHEMA2], and WSDL as defined in [WSDL].

2.2.1 Namespaces

This protocol uses the namespaces listed in the [MS-OAUTH2EX] OAuth 2.0 Authentication Protocol Extensions specification.

3 Protocol Details

3.1 Server Role Details

Following lists the end to end flow for a sample scenario that involves server to server authentication when an application calls to SharePoint.

1. Application makes an anonymous service call to SharePoint
2. SharePoint returns a HTTP 401 challenge
3. Application creates a S2S token that contains the user identity information as an outer token
4. Application sends the S2S token, which has augmented user information, to the SharePoint
5. SharePoint validates the S2S token and extracts the user identity information

This section describes the profile in details.

This profile is applied for the following SharePoint end points:

Client.svc

Listdata.svc

Sites.asmx

_api

Realm discovery through 401 challenge

This is step 2 in the end-to-end flow provided at the beginning of this section.

SharePoint responds with 401 challenges for the anonymous requests made to the resource end points with an empty 'Bearer' authorization header. 'Bearer' authorization header is specified in [IETFDRAFT-JWT] JSON Web Token specification.

The response contains the following two parameters:

- client_id
  - application identifier, the value is 00000003-0000-0ff1-ce00-000000000000
- realm
  - the source realm of the application. The format of realm is specified in the [MS-OAUTH2EX] OAuth 2.0 Authentication Protocol Extensions.

S2S Token Contents for this profile

The S2S token sent by the application MUST be compatible with JSON web token format specified in the [IETFDRAFT-JWT] JSON Web Token and [MS-OAUTH2EX] OAuth 2.0 Authentication Protocol Extensions.

This is the step 4 in the end-to-end flow provided at the beginning of this section.

SharePoint accepts S2S tokens with the following claims. All the claims are of data type 'string' unless otherwise specified:

Claim type (description)	Claim value description	Possible/Example claim values
aud (audience)	Targeted service for which the token is issued. The format of this value is described in the [MS-OAUTH2EX] OAuth 2.0 Authentication Protocol Extensions. For example, if the token is intended for SharePoint instance then the value is microsoft.sharepoint/<hostname>@<realm>	00000003-0000-0ff1-ce00-000000000000/<hostname>@<realm>
iss (issuer)	The principal of the issuer. The format of this value is described in the [MS-OAUTH2EX] OAuth 2.0 Authentication Protocol Extensions.	<principal PID>@<realm>
nid (name identifier)	The value of the principal that makes the request. The format of this value is described in the [MS-OAUTH2EX] OAuth 2.0 Authentication Protocol Extensions.	Signed in user's UPN value Example: contoso\user
nbf (not_before)	Time at which the token was created. The format of this value is described in the [MS-OAUTH2EX] OAuth 2.0 Authentication Protocol Extensions.	Example value: 129592882368666656
exp (expires_on)	Time at which the token expires. The format of this value is described in the [MS-OAUTH2EX] OAuth 2.0 Authentication Protocol Extensions.	Example value: 129592882368666656
trustedfordelegation	Value indicating whether the caller is trusted to delegate a user identity. The format of this value is described in the [MS-OAUTH2EX] OAuth 2.0 Authentication Protocol Extensions.	true false
Identityprovider	String value indicating the identity provider who authenticated the caller. This is an additional claim that SharePoint accepts and not required by [MS-OAUTH2EX] OAuth 2.0 Authentication Protocol Extensions.	windows accesstoken
actortoken	This value points to the security token issued and signed by a trusted issuer. The format of this value is described in the [MS-OAUTH2EX] OAuth 2.0 Authentication Protocol Extensions.	
smtp	The logged on user's email address. This is an additional claim that trusted issuers shall send and it expected to be a string value.	Claim value depends on what is configured as email address for the user. Example: user@contoso.com

Claim type (description)	Claim value description	Possible/Example claim values
sip	The logged on user's sip address. This is an additional claim that trusted issuers shall send and it expected to be a string value.	Claim value depends on what is configured as sip address for the user. Example: sip:user@contoso.com

S2S token validation criteria

This is step 5 in the end-to-end flow provided at the beginning of this section.

The relying party application accepts S2S tokens as long as the following criteria are met:

- Token is signed with one of SharePoint's trusted signing certificates
- Token contains at least one of the following claims:
  - nid claim with the UPN value
  - smtp claim
  - sip claim
- iss claim value in the outer token matches nid claim value in the inner token; case sensitive comparison is performed
- aud claim value succeeds the audience validation check which includes the following:
  - aud claim MUST contain three parts, client_id, authority, and realm
  - client_id is 00000003-0000-0ff1-ce00-000000000000
  - authority is the host name of the SharePoint's end point
  - realm matches the requested resource's realm

SharePoint uses the claims in the token to look up a user profile against its internal database and then continue its internal operations to authorize the caller.

3.1.1 Abstract Data Model

None

3.1.2 Timers

None

3.1.3 Initialization

This profile sequence is initiated when a server to server authentication call starts.

3.1.4 Higher-Layer Triggered Events

None

3.1.5 Message Processing Events and Sequencing Rules

None.

3.1.6 Timer Events

None

3.1.7 Other Local Events

None

3.2 Client Role Details

Following lists the end to end flow for a sample scenario that involves server to server authentication when SharePoint makes a call to another application that is compatible with the server to server authentication protocol as specified in [MS-OAUTH2EX] OAuth 2.0 Authentication Protocol Extensions.

Note that this flow is adapted for SharePoint to Exchange and SharePoint to Lync communications as well.

1. SharePoint makes an anonymous service call to the relying party service
2. Relying Party (RP) service returns a HTTP 401 challenge
3. SharePoint creates a S2S token with user identity information augmented to it as an outer token.
4. SharePoint sends the S2S token, which has augmented user information, to the relying party service.
5. Relying party service validates the S2S token and extracts the user identity information.

SharePoint makes service calls to the relying party application

SharePoint makes anonymous calls to the relying party application with empty value in 'Bearer' authentication scheme as specified in [IETFDRAFT-JWT] JSON Web Token specification.

Realm auto discovery through 401 challenges

This is step 2 in the end-to-end flow provided at the beginning of this section.

The relying party application responds with 401 challenges.

This response contains the following two optional parameters:

- client_id
  - application identifier, in the case of SharePoint as an application this value is 00000003-0000-0ff1-ce00-000000000000
- realm
  - the realm of the application end point. The format of realm is specified in the [MS-OAUTH2EX] OAuth 2.0 Authentication Protocol Extensions

SharePoint S2S Token Contents

This is step 3 in the end-to-end flow provided at the beginning of this section.

All the claims issued by SharePoint are of data type 'string' and the token is signed with the private key of its signing certificate.

Claim type (description)	Claim value description	Possible/Example claim values
aud (audience)	Targeted service for which the token is issued. The format of this value is described in the [MS-OAUTH2EX] OAuth 2.0 Authentication Protocol Extensions.	00000002-0000-0ff1-ce00-000000000000@<realm> 00000004-0000-0ff1-ce00-000000000000@<realm>
iss (issuer)	The principal of the issuer. The format of this value is described in the [MS-OAUTH2EX] OAuth 2.0 Authentication Protocol Extensions.	microsoft.sharepoint@<realm>
nid (name identifier)	The value of the principal that makes the request. The format of this value is described in the [MS-OAUTH2EX] OAuth 2.0 Authentication Protocol Extensions.	microsoft.sharepoint@realm
nbf (not_before)	Time at which the token was created. The format of this value is described in the [MS-OAUTH2EX] OAuth 2.0 Authentication Protocol Extensions.	The following is only a sample value: 129592882368666656
exp (expires_on)	Time at which the token expires. The format of this value is described in the [MS-OAUTH2EX] OAuth 2.0 Authentication Protocol Extensions.	The following is only a sample value: 129592882368666656
trustedfordelegation	Value indicating whether the caller is trusted to delegate a user identity. The format of this value is described in the [MS-OAUTH2EX] OAuth 2.0 Authentication Protocol Extensions.	true false
Identityprovider	String value indicating the identity provider who authenticated the caller. This is an additional claim that SharePoint issues and not required by [MS-OAUTH2EX] OAuth 2.0 Authentication Protocol Extensions.	windows forms trusted

Augmenting user identity information

Application adds the currently logged on users identity information as an outer token to the S2S token. This allows the application to convey the user information to the relying party service.

This outer token SHALL contain following claims:

Claim type	Claim value description	Possible/Example claim values
aud (audience)	Targeted service for which the token is intended for. The format of this value is described in the [MS-OAUTH2EX] OAuth 2.0 Authentication Protocol Extensions.	00000002-0000-0ff1-ce00-000000000000/<hostname:port>@<realm> 00000004-0000-0ff1-ce00-000000000000microsoft.lync/<hostname:port>@<realm>
iss (issuer)	The principal of the issuer. The format of this value is described in the [MS-OAUTH2EX] OAuth 2.0 Authentication Protocol Extensions.	microsoft.sharepoint@<realm>
nid (name identifier)	The logged on user's UPN value of the principal that makes the request. The format of this value is described in the [MS-OAUTH2EX] OAuth 2.0 Authentication Protocol Extensions.	Claim value depends on what is configured as UPN for the user. Example: contoso\user
Identityprovider	String value indicating the identity provider who authenticated the caller. This is an additional claim that SharePoint issues and not required by [MS-OAUTH2EX] OAuth 2.0 Authentication Protocol Extensions.	windows forms trusted
smtp	The logged on user's email address. This is an additional claim that SharePoint adds and not required by [MS-OAUTH2EX] OAuth 2.0 Authentication Protocol Extensions.	Claim value depends on what is configured as email address for the user. Example: user@contoso.com
actortoken	This value points to the inner token. The format of this value is described in	This contains the claims of inner token called out in the preceding section.

Claim type	Claim value description	Possible/Example claim values
	the [MS-OAUTH2EX] OAuth 2.0 Authentication Protocol Extensions.	

SharePoint accepts serialized user information that is a JSON encoded key-value pair like below in order to make an outgoing S2S call.

{"typ":1,"idk":"bmFtZWlkDQpkdGF5bG9yQG1pY3Jvc29mdC5jb20NCg==","idp":"windows"}

"typ" is the token type, where value of 1 indicates that the information is for an application & user identities whereas value of 2 indicates that the information is for application only identity.

"idk" is the Base64 encoded identity key. This key is returned by an identity resolver that is shared by the client and server components. For example, SharePoint has an built-in identity resolver User Profile Application.

"idp" is the identity provider claim. Possible values of this claim are: windows, forms, and trusted.

3.2.1 Abstract Data Model

None

3.2.2 Timers

None

3.2.3 Initialization

This profile sequence is initiated when a server to server authentication call starts.

3.2.4 Higher-Layer Triggered Events

None

3.2.5 Message Processing Events and Sequencing Rules

None.

3.2.6 Timer Events

None

3.2.7 Other Local Events

None

4 Protocol Examples

4.1 Sample S2S token when making outbound calls from an application that adheres to this profile

```
{
    iss: 00000003-0000-0ff1-ce00-000000000000@contoso.com
    nameid: 00000003-0000-0ff1-ce00-000000000000@contoso.com
    identityprovider: 00000003-0000-0ff1-ce00-000000000000@contoso.com
    nbf: 1320176785
    exp: 1320219985
    aud: 00000003-0000-0ff1-ce00-000000000000/mysite.contoso.com@contoso.com
    trustedfordelegation: true
}
{
    iss: 00000003-0000-0ff1-ce00-000000000000@contoso.com
    nameid: user@contoso.com
    identityprovider: windows
    nbf: 1320176785
    exp: 1320219985
    aud: 00000003-0000-0ff1-ce00-000000000000/mysite.contoso.com@contoso.com
    actortoken:
    {
        iss: 00000003-0000-0ff1-ce00-000000000000@contoso.com
        nameid: 00000003-0000-0ff1-ce00-000000000000@contoso.com
        identityprovider: 00000003-0000-0ff1-ce00-000000000000@contoso.com
        nbf: 1320176785
        exp: 1320219985
        aud: 00000003-0000-0ff1-ce00-000000000000/mysite.contoso.com@contoso.com
        trustedfordelegation: true
    }
}
```

5 Security

5.1 Security Considerations for Implementers

Security considerations mentioned in the following specifications should be considered when implementing this profile.

- Section 10 in [IETFDRAFT-OAuth2.0] OAuth 2.0 Authentication Protocol
- Section 10 in [IETFDRAFT-JWT] JSON Web Token Specification
- Security considerations section in [MS-OAUTH2EX] OAuth 2.0 Authentication Protocol Extensions document

In addition following security aspects should be considered:

- Access tokens issued by the Security Token Service are Bearer tokens and must be kept confidential in transit and in storage. It is recommended to use TLS (SSL) secured channel for transmitting the access tokens.
- Since the augmented user identity information in the outer token is not signed by the application and the receiver of the S2S token should validate that the value of the trustedForDelegation claim is set to true.
- The receiver of the S2S token should validate that the aud (audience) claim in the inner and outer token match. Also, it should ensure that the token is intended for itself by ensuring that the aud claim contains its hostname.

5.2 Index of Security Parameters

None

6 Appendix A: Product Behavior

The information in this specification is applicable to the following Microsoft products or supplemental software. References to product versions include released service packs:

- Microsoft® SharePoint® Server 15 Technical Preview
- Microsoft® SharePoint® Foundation 15 Technical Preview

Exceptions, if any, are noted below. If a service pack or Quick Fix Engineering (QFE) number appears with the product version, behavior changed in that service pack or QFE. The new behavior also applies to subsequent service packs of the product unless otherwise specified. If a product edition appears with the product version, behavior is different in that product edition.

Unless otherwise specified, any statement of optional behavior in this specification that is prescribed using the terms SHOULD or SHOULD NOT implies product behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term MAY implies that the product does not follow the prescription.

7 Change Tracking

No table of changes is available. The document is either new or has had no changes since its last release.

8 Index