[MS-OAUTH2EX]:

OAuth 2.0 Authentication Protocol Extensions

Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation ("this documentation") for protocols, file formats, data portability, computer languages, and standards support. Additionally, overview documents cover inter-protocol relationships and interactions.
- **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 can make copies of it in order to develop implementations of the technologies that are described in this documentation and can distribute portions of it in your implementations that use these technologies or in your documentation as necessary to properly document the implementation. You can also distribute in your implementation, with or without modification, any schemas, IDLs, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications documentation.
- **No Trade Secrets**. Microsoft does not claim any trade secret rights in this documentation.
- **Patents**. Microsoft has patents that might cover your implementations of the technologies described in the Open Specifications documentation. Neither this notice nor Microsoft's delivery of this documentation grants any licenses under those patents or any other Microsoft patents. However, a given Open Specifications document might be covered by the Microsoft Open Specifications Promise or the Microsoft Community Promise. If you would prefer a written license, or if the technologies described in this documentation 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 might be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights. For a list of Microsoft trademarks, visit www.microsoft.com/trademarks.
- **Fictitious Names**. The example companies, organizations, products, domain names, email addresses, logos, people, places, and events that are 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 as specifically described above, whether by implication, estoppel, or otherwise.

Tools. The Open Specifications documentation does 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 documents are intended for use in conjunction with publicly available standards specifications and network programming art and, as such, assume that the reader either is familiar with the aforementioned material or has immediate access to it.

Revision Summary

Date	Revision History	Revision Class	Comments
1/20/2012	0.1	New	Released new document.
4/11/2012	0.1	None	No changes to the meaning, language, or formatting of the technical content.
7/16/2012	0.1	None	No changes to the meaning, language, or formatting of the technical content.
9/12/2012	0.1	None	No changes to the meaning, language, or formatting of the technical content.
10/8/2012	1.0	Major	Significantly changed the technical content.
2/11/2013	1.0	None	No changes to the meaning, language, or formatting of the technical content.
7/30/2013	1.0	None	No changes to the meaning, language, or formatting of the technical content.
11/18/2013	1.0	None	No changes to the meaning, language, or formatting of the technical content.
2/10/2014	1.0	None	No changes to the meaning, language, or formatting of the technical content.
4/30/2014	1.1	Minor	Clarified the meaning of the technical content.
7/31/2014	1.1	None	No changes to the meaning, language, or formatting of the technical content.
10/30/2014	1.1	None	No changes to the meaning, language, or formatting of the technical content.
3/16/2015	2.0	Major	Significantly changed the technical content.
2/26/2016	3.0	Major	Significantly changed the technical content.
7/15/2016	3.0	None	No changes to the meaning, language, or formatting of the technical content.

Table of Contents

1 Introduction 4
1.1 Glossary 4
1.2 References 5
1.2.1 Normative References 5
1.2.2 Informative References 5
1.3 Overview 6
1.4 Relationship to Other Protocols 6
1.5 Prerequisites/Preconditions 6
1.6 Applicability Statement 6
1.7 Versioning and Capability Negotiation 6
1.8 Vendor-Extensible Fields 6
1.9 Standards Assignments 6

2 Messages 7
2.1 Transport 7
2.2 Message Syntax 7
2.2.1 Common URI Parameters 7

3 Protocol Details 9
3.1 Common Details 9
3.1.1 Abstract Data Model 9
3.1.2 Timers 9
3.1.3 Initialization 9
3.1.4 Higher-Layer Triggered Events 9
3.1.5 Message Processing Events and Sequencing Rules 9
3.1.5.1 Protected Resource 9
3.1.5.1.1 Request Access 9
3.1.5.1.1.1 Request Body 9
3.1.5.1.1.2 Response Body 9
3.1.5.1.1.3 Processing Details 9
3.1.6 Timer Events 9
3.1.7 Other Local Events 10

4 Protocol Examples 11
4.1 Example request for token to access a resource 11
4.2 Response with token to access requested resource 11

5 Security 12
5.1 Security Considerations for Implementers 12
5.2 Index of Security Parameters 12

6 Appendix A: Full JSON Schema 13

7 Appendix B: Product Behavior 14

8 Change Tracking 15

9 Index 16

1 Introduction

OAuth 2.0 Authentication Protocol Extensions describes extensions to the OAuth 2.0 Authentication Protocol. These extensions consist of additional parameters in the request **URI** and the **JSON** objects returned in the **HTTP** response body.

Sections 1.5, 1.8, 1.9, 2, and 3 of this specification are normative. All other sections and examples in this specification are informative.

1.1 Glossary

This document uses the following terms:

Coordinated Universal Time (UTC): A high-precision atomic time standard that approximately tracks Universal Time (UT). It is the basis for legal, civil time all over the Earth. Time zones around the world are expressed as positive and negative offsets from UTC. In this role, it is also referred to as Zulu time (Z) and Greenwich Mean Time (GMT). In these specifications, all references to UTC refer to the time at UTC-0 (or GMT).

Hypertext Transfer Protocol (HTTP): An application-level protocol for distributed, collaborative, hypermedia information systems (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.

Hypertext Transfer Protocol Secure (HTTPS): An extension of HTTP that securely encrypts and decrypts web page requests. In some older protocols, "Hypertext Transfer Protocol over Secure Sockets Layer" is still used (Secure Sockets Layer has been deprecated). For more information, see [SSL3] and [RFC5246].

JavaScript Object Notation (JSON): A text-based, data interchange format that is used to transmit structured data, typically in Asynchronous JavaScript + XML (AJAX) web applications, as described in [RFC4627]. The JSON format is based on the structure of ECMAScript (Jscript, JavaScript) objects.

principal: An authenticated entity that initiates a message or channel in a distributed system.

realm: An administrative boundary that uses one set of authentication servers to manage and deploy a single set of unique identifiers. A realm is a unique logon space.

Representational State Transfer (REST): A class of web services that is used to transfer domain-specific data by using **HTTP**, without additional messaging layers or session tracking, and returns textual data, such as XML.

security token: An opaque message or data packet produced by a Generic Security Services (GSS)-style authentication package and carried by the application protocol. The application has no visibility into the contents of the **token**.

security token service (STS): A web service that issues claims (2) and packages them in encrypted security tokens.

tenant: A protocol client or protocol server that accesses a partition in a shared service database.

token: A word in an item or a search query that translates into a meaningful word or number in written text. A token is the smallest textual unit that can be matched in a search query. Examples include "cat", "AB14", or "42".

Transmission Control Protocol (TCP): A protocol used with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. TCP handles keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

Uniform Resource Identifier (URI): A string that identifies a resource. The URI is an addressing mechanism defined in Internet Engineering Task Force (IETF) Uniform Resource Identifier (URI): Generic Syntax [RFC3986].

Uniform Resource Locator (URL): A string of characters in a standardized format that identifies a document or resource on the World Wide Web. The format is as specified in [RFC1738].

X.509: An ITU-T standard for public key infrastructure subsequently adapted by the IETF, as specified in [RFC3280].

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

1.2 References

Links to a document in the Microsoft Open Specifications library point to the correct section in the most recently published version of the referenced document. However, because individual documents in the library are not updated at the same time, the section numbers in the documents may not match. You can confirm the correct section numbering by checking the Errata.

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.

[IETFDRAFT-JWT-LATEST] Jones, M., Bradley, J., and Sakimura, N., "JSON Web Token (JWT) draft-ietf-oauth-json-web-token-08", draft-ietf-oauth-json-web-token-08, May 2013, http://datatracker.ietf.org/doc/draft-ietf-oauth-json-web-token/

[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-SPS2SAUTH] Microsoft Corporation, "OAuth 2.0 Authentication Protocol: SharePoint Profile".

[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

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000, http://www.rfc-editor.org/rfc/rfc2818.txt

[RFC3986] Berners-Lee, T., Fielding, R., and Masinter, L., "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005, http://www.ietf.org/rfc/rfc3986.txt

[RFC793] Postel, J., Ed., "Transmission Control Protocol: DARPA Internet Program Protocol Specification", RFC 793, September 1981, http://www.rfc-editor.org/rfc/rfc793.txt

1.2.2 Informative References

[MS-OXPROTO] Microsoft Corporation, "Exchange Server Protocols System Overview".

[MS-XOAUTH] Microsoft Corporation, "OAuth 2.0 Authorization Protocol Extensions".

[RFC2616] Fielding, R., Gettys, J., Mogul, J., et al., "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999, http://www.rfc-editor.org/rfc/rfc2616.txt

1.3 Overview

This document describes extensions to the OAuth 2.0 Authentication Protocol. These extensions consist of additional parameters in the request URI and the JSON objects returned in the HTTP response body, as described in [RFC2616]. These extensions provide additional functionality, such as finer granularity of token expiry periods, which is incremental over what is provided by the base specification.

1.4 Relationship to Other Protocols

This protocol extends and relies on the **OAuth 2.0 Authentication Protocol**, as specified by [MS-SPS2SAUTH]. This protocol is related to the **OAuth 2.0 Authorization Protocol Extensions** as described in [MS-XOAUTH].

For conceptual background information and overviews of the relationships and interactions between this and other protocols, see [MS-OXPROTO].

1.5 Prerequisites/Preconditions

Applications using these extensions will have their **principal** identifiers registered as members of the **realm** managed by the **security token service (STS)** and are able to authenticate to it by exchanging secrets (public key material carried in **X.509** certificates). The applications will also trust tokens issued by the STS. These preconditions are established during deployment of new **tenants**.

1.6 Applicability Statement

These extensions are used in OAuth 2.0 Authentication requests for obtaining an access **token** for use with **REST** bases service requests.

1.7 Versioning and Capability Negotiation

None.

1.8 Vendor-Extensible Fields

None.

1.9 Standards Assignments

None.

2 Messages

2.1 Transport

This protocol transports messages over **TCP**, as specified in [RFC793], and does not pass any specific parameters to the transport. This protocol uses **HTTPS**, as specified in [RFC2818], to secure the **security tokens**.

2.2 Message Syntax

Parameters in these extensions are either transmitted in the request body in **URL**-encoded form or in the response as part of a JSON object. Tokens returned in conjunction with use of this protocol conform to the JSON Web Token (JWT) specification [IETFDRAFT-JWT-LATEST].

XML based serialization is not used with these extensions or underlying protocols.

2.2.1 Common URI Parameters

The following parameters are used in conjunction with the OAuth 2.0 Authentication Protocol, as specified in [MS-SPS2SAUTH]:

URI Parameter	Type	Location/Usage	Description
Resource	string, URI value expected	Request body, URL-encoded	Indicates the target resource that the caller wants to talk to. Value is expected to be URI format as defined in [RFC3986]. This parameter MUST be present.
not_before	string, URI value expected	Response body in JSON object	A token returned in the OAuth parameter *access_token*, as specified in [IETFDRAFT-OAuth2.0], as part of this response is not valid before the time specified in this parameter. This parameter MUST be present.
expires_on	string, **UTC** value expected	Response body in JSON object	A token returned in the OAuth parameter *access_token* as part of this response will no longer be valid at the time specified in this parameter. This parameter MUST be present.
realm	string, URI value expected	Request body, URL-encoded or Response body in JSON object	Indicates the realm that the caller is part of. This parameter is optional.
created_on	string, UTC value expected	Request body, URL-encoded or Response body in JSON object	A token returned in the OAuth parameter *access_token* as part of this was created at the time specified in this parameter. This parameter is optional.
expires_in	string, int value expected	Response body in JSON object	The lifetime of the token returned in the OAuth parameter *access_token* as part of this response

URI Parameter	Type	Location/Usage	Description
			specified in seconds. This parameter is optional.

3 Protocol Details

3.1 Common Details

This specification defines additional parameters for use with OAuth 2.0 Authentication Protocol messages specified in [MS-SPS2SAUTH].

These parameters convey additional semantics related to the access token being requested and about the access token returned as part of these messages. This specification does not define any additional messages over the base specification.

3.1.1 Abstract Data Model

3.1.2 Timers

None.

3.1.3 Initialization

Connections made using the underlying OAuth 2.0 Authentication Protocol (specified in [MS-SPS2SAUTH]) are what initiate use of the extensions defined in this specification.

3.1.4 Higher-Layer Triggered Events

None.

3.1.5 Message Processing Events and Sequencing Rules

The token request contains the elements indicated in section 3.1.1.

3.1.5.1 Protected Resource

This resource indicates the protected resource that the user is trying to get access to.

3.1.5.1.1 Request Access

For gaining access to a resource, an access token with the elements mentioned in section 3.1.1 need to be presented.

3.1.5.1.1.1 Request Body

Refer to the section 4.1.

3.1.5.1.1.2 Response Body

Refer to the section 4.2.

3.1.5.1.1.3 Processing Details

None.

3.1.6 Timer Events

None.

3.1.7 Other Local Events

None.

4 Protocol Examples

4.1 Example request for token to access a resource

The following is an example request for token to access a resource:

```
POST https://example.com/tokens/OAuth/2 HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: example.com
Content-Length: 660
Expect: 100-continue
grant type=http%3a%2f%2foauth.net%2fgrant type%2fjwt%2f1.0%2fbearer&assertion=eyJ0eXAiOiJKV1Q
iLCJhbGciOiJSUzI1NiIsIng1dCI6IkM5Qi1lUHpvYnVtejVoM3lZb3FJbjhHWFFwNCJ9.eyJhdWQiOiIwMDAwMDAwMS0
wMDAwLTAwMDAtYzAwMC0wMDAwMDAwMDAwMDAvc3RzLWludC1zbjEtMDAzLmFjY2Vzc2NvbnRyb2wuYWFkaW50LndpbmRv
d3MtaW50Lm5ldEBtZ29vZG5lci5jb20iLCJpc3MiOiJDTj1BQ1MyQ2xpZW50Q2VydGlmaWNhdGVAbWdvb2RuZXIuY29tI
iwibmJmIjoiMTMyMTY1NTMzOSIsImV4cCI6IjEzMjE2NTg5MzkifQ.XcO8kUte4PKjPwpmXiTBKo4bDAAVJW1eB9d69nM
paumjl9vqw-
N0wLIDN4M6btn_G1BYgcPh0l3hl7Lsxs7E2SfssIegY_KuHZJIdb3pyc0KNzfcoolxIZRFQDK3zmYKICBEQCJ9nHBLcL4
Y8AXkZVddYjGo-104M4rg0AcXMZU&resource=example.com/resouce
```

4.2 Response with token to access requested resource

The following is an example of a response with token to access the requested resource:

```
HTTP/1.1 200 OK
Cache-Control: public, no-store, max-age=0
Pragma: no-cache
Content-Type: application/json; charset=utf-8
Expires: Fri, 18 Nov 2011 22:28:59 GMT
Last-Modified: Fri, 18 Nov 2011 22:28:59 GMT
Vary: *
Server: Microsoft-IIS/7.5
Set-Cookie: ASP.NET SessionId=5v3qtoiaxr3m21gdbbai0cxu; path=/; HttpOnly
X-AspNetMvc-Version: 2.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
X-Content-Type-Options: nosniff
Date: Fri, 18 Nov 2011 22:28:59 GMT
Content-Length: 1146
{
"access_token":"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ilhxcm5GRWZzUzU1X3ZNQnBIdkYwcFRuc
WVhTSJ9.eyJhdWQiOiJtaWNyb3NvZnQuZXhjaGFuZ2UvbG9jYWxob3N0OjQ1NzA0QEVENjhGQTczLTNCRTYtNDYxMi1BO
TQ0LTI3ODY1OUVEOTAwNCIsImlzcyI6IjAwMDAwMDAxLTAwMDAtMDAwMC1jMDAwLTAwMDAwMDAwMDAwMEBFRDY4RkE3My
0zQkU2LTQ2MTItQTk0NC0yNzg2NTlFRDkwMDQiLCJuYmYiOjEzMjE2NTUzNDAsImV4cCI6MTMyMTY1ODk0MCwibmFtZWl
kIjoiQ049QUNTMkNsaWVudENlcnRpZmljYXRlQEVENjhGQTczLTNCRTYtNDYxMi1BOTQ0LTI3ODY1OUVEOTAwNCIsImlk
ZW50aXR5cHJvdmlkZXIiOiIwMDAwMDAwMS0wMDAwLTAwMDAtYzAwMC0wMDAwMDAwMDAwMDBARUQ2OEZBNzMtM0JFNi00N
jEyLUE5NDQtMjc4NjU5RUQ5MDA0In0.j0KHTj0VGKN35-
NOLnN14MWOrUzKcWKXXCwOzj6LFZNrBgEBzIUvSksZ9Av4nxB_wYzflp9QEFDOMUkSkzlBt4t4eUZxbb78RSMHJLnetnL
CUgL7POuE4e_-x3kq_LNnYc_-VQ9MLw4KIblwJrVD4LyMNVlo-5VGIybKMGM3fVvtrazgvgFC-
7MmQbmjJ8m249J8InL7Qt2fbyBuPRA0Ey9LhLDqZ7t LWUGc ufNxP7T0crzSun6MhUM332-
lW7OFdq6HXx1oD6qDc8te5cQ9IloF6WYonDTiCBCxfiTt-ouEHskOZDwZ781wBTn9TJujMYo1vjurXUVqiBNZCQ-A",
"token_type":"http://oauth.net/grant_type/jwt/1.0/bearer",
"expires_in":"3599",
"scope":"example.com/resource@guid",
"not_before":"1321655340",
"expires on":"1321658940"
}
```

5 Security

5.1 Security Considerations for Implementers

It is recommended that security considerations described in underlying specifications and in profiles referencing this extension specification be considered when using these extensions.

5.2 Index of Security Parameters

None.

6 Appendix A: Full JSON Schema

For ease of implementation, the following is the full JSON schema for this protocol.

```
"not_before" : {
"type" : "string",
"format" : "date-time"
},
"expires_on" : {
"type" : "string",
"format" : "date-time"
},
"realm" : {
"type" : "string",
"format" : "uri"
},
"created on" : {
"type" : "string",
"format" : "date-time"
},
"expires in" : {
"type" : "integer"
}
```

7 Appendix B: 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 Lync Client 2013/Skype for Business
- Microsoft Lync Server 2013
- Microsoft Exchange Server 2013
- Microsoft SharePoint Server 2013
- Microsoft SharePoint Foundation 2013
- Microsoft Skype for Business 2016
- Microsoft Skype for Business Server 2015
- Microsoft SharePoint Server 2016

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.

8 Change Tracking

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

9 Index

A

Abstract data model:common
  Data model – abstract:common 9
Applicability 6

C

Capability negotiation 6
Change tracking 15
Common
  Higher-layer triggered events 9
  Initialization 9
  Message processing events and sequencing rules 9
  Other local events 10
  Timer events 9
  Timers 9
Common:message processing
  Common:sequencing rules 9

E

Examples
  Example request for token to access a resource example 11
  Response with token to access requested resource example 11

F

Fields - vendor-extensible 6
Full JSON schema 13

G

Glossary 4

I

Implementer - security considerations 12
Index of security parameters 12
Informative references 5
Initialization:common
  Common:initialization 9
Introduction 4

J

JSON schema 13

M

Messages
  transport 7
Messages:syntax
  Syntax:messages - overview 7
Messages:transport
  Transport 7

N

Normative references 5

O

Overview (synopsis) 6

P

Parameters - security index 12
Preconditions 6
Prerequisites 6
Product behavior 14
Protocol Details
  Common 9
Protocol examples
  Example request for token to access a resource 11
  Response with token to access requested resource 11

R

References
  informative 5
  normative 5
Relationship to other protocols 6
Request for token to access a resource example
  Example:Request for token to access a resource 11
Response with token to access requested example
  Example:Response with token to access requested resource 11

S

Security
  implementer considerations 12
  parameter index 12
Standards assignments 6

T

Tracking changes 15
Transport 7

V

Vendor-extensible fields 6
Versioning 6

X

XML schema
  Full XML schema 13