OAuth 2 Vocabulary

Release 30 Juni 2017

This version:
http://www.daspsec.org/o/oauth-2.0/0.2

Revision:
0.2

Authors:
Bojan Suzic, (Graz University of Technology)

Publisher:
A-SIT Secure Information Technology Center - Austria

Download serialization:

Format RDF/XML Format N Triples Format TTL

Abstract

This document proposes a vocabulary for modeling OAuth 2.0 based interactions and entities. It is currently in draft phase and aims at non-complete coverage of the concepts that are relevant for its application in DASP framework.

Table of contents

1. Introduction

back to ToC

Simplicity, clarity of the structure and its relationship with underlying standards and technologies are some of the factors that allowed RESTful architectural style to become broadly adopted approach in exposing web services. Today, significant portion of the service-based intra and inter-domain interactions rely on Web APIs. OAuth 2.0 web authorization framework is one of de facto dominant approaches used to secure access to such APIs. In this document we provide a proposal of a vocabulary that describes the interactions and entities present in OAuth 2.0 framework. The primary purpose of this vocabulary is to facilitate the use cases present in DASP framework for cross-organizational context-aware authorization management. By relying on the concepts from this vocabulary, other components of DASP framework are able to specify, integrate, reason over and evaluate the client capabilities and derive authorization decisions for interactions intercepted in the scope of cross-domain authorization management and enforcement. The purpose of this vocabulary is furthermore to facilitate OAuth 2.0 application and integration with other tools and frameworks beyond this specific project or use case.

1.1. Namespace declarations

Table 1: Namespaces used in the document

ns	<http://creativecommons.org/ns#>
owl	<http://www.w3.org/2002/07/owl#>
oauth-2-0	<http://www.daspsec.org/o/oauth-2.0/>
dasp-interaction	<http://www.daspsec.org/o/dasp-interaction/>
xsd	<http://www.w3.org/2001/XMLSchema#>
rdfs	<http://www.w3.org/2000/01/rdf-schema#>
o	<http://www.daspsec.org/o/>
rdf	<http://www.w3.org/1999/02/22-rdf-syntax-ns#>
terms	<http://purl.org/dc/terms/>
files	<https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/>
html	<https://tools.ietf.org/html/>
vann	<http://purl.org/vocab/vann/>
dc	<http://purl.org/dc/elements/1.1/>

2. OAuth 2 Vocabulary: Overview

back to ToC

This ontology has the following classes and properties.

Classes

Access Token Authorization Endpoint Authorization Request Authorization Response Authorization Server Bearer Token Client Endpoint Error Response Redirection Endpoint Refresh Token Resource Owner Resource Server Token Token Endpoint

Object Properties

hasEndpoint

Data Properties

hasBearerTokenValue hasClientIdentifier hasClientPassword hasDesiredGrantType hasEndpointURI hasRefreshTokenValue hasTokenValue

3. OAuth 2 Vocabulary: Description

back to ToC

The current version of this vocabulary supports the concepts and relationships that are necessary to perform and evaluate minimalistic use cases from DASP framework. Please note that this is ongoing draft and may be extended in the future releases or inception of new use cases.

4. Cross reference for OAuth 2 Vocabulary classes, properties and dataproperties

back to ToC

This section provides details for each class and property defined by OAuth 2 Vocabulary.

4.1. Classes

Access Token[C]

back to ToC or Class ToC

IRI: http://www.daspsec.org/o/oauth-2.0#AccessToken

Credential used to access protected resource represented as a string that specifies scopes and durations of access granted by the resource owner.

has super-classes

Token [c]

has sub-classes

Bearer Token [c]

Authorization Endpoint[C]

back to ToC or Class ToC

IRI: http://www.daspsec.org/o/oauth-2.0#AuthorizationEndpoint

An endpoint used by the client to obtain authorization from the resource owner via user-agent redirection.

has super-classes

Endpoint [c]

Authorization Request[C]

back to ToC or Class ToC

IRI: http://www.daspsec.org/o/oauth-2.0#AuthorizationRequest

A request constructed by the client and provided to the resource owner with the purpose of obtaining an authorization code.

has super-classes

request [c]

is in domain of

hasDesiredGrantType [dp]

Authorization Response[C]

back to ToC or Class ToC

IRI: http://www.daspsec.org/o/oauth-2.0#AuthorizationResponse

A response generated by authorization server and sent to the client following the successfull authorization consented by the resource owner.

has super-classes

response [c]

Authorization Server[C]

back to ToC or Class ToC

IRI: http://www.daspsec.org/o/oauth-2.0#AuthorizationServer

The server that issues access tokens to the client after successfully authenticating the resource owner and obtaining authorization or consent.

has super-classes
thing [c]

Bearer Token[C]

back to ToC or Class ToC

IRI: http://www.daspsec.org/o/oauth-2.0#BearerToken

A security credential with the property that any party in its posession can use the credential in any way any other party in possession of it can. Using a bearer token does not require a bearer to prove possession of cryptographic key material (proof-of-possession).

has super-classes
Access Token [c]

Client[C]

back to ToC or Class ToC

IRI: http://www.daspsec.org/o/oauth-2.0#OAuthClient

An application or agent that initiates request to protected resource on behalf of resource owner.

has super-classes
access client [c]
is in domain of
hasBearerTokenValue [dp], hasClientIdentifier [dp], hasClientPassword [dp], hasRefreshTokenValue [dp]

Endpoint[C]

back to ToC or Class ToC

IRI: http://www.daspsec.org/o/oauth-2.0#Endpoint

An URI-based location that is used to perform message exchanges between clients and endpoint holders.

has super-classes
thing [c]
has sub-classes
Authorization Endpoint [c], Redirection Endpoint [c], Token Endpoint [c]
is in range of
hasEndpoint [op]

Error Response[C]

back to ToC or Class ToC

IRI: http://www.daspsec.org/o/oauth-2.0#ErrorResponse

A response generated by authorization server and provided to the client following the failed authorization request.

has super-classes
response [c]

Redirection Endpoint[C]

back to ToC or Class ToC

IRI: http://www.daspsec.org/o/oauth-2.0#RedirectionEndpoint

An endpoint used by the authorization server to return responses containing authorization credentials to the client via the resource owner user-agent.

has super-classes
Endpoint [C]

Refresh Token[C]

back to ToC or Class ToC

IRI: http://www.daspsec.org/o/oauth-2.0#RefreshToken

Credential used to obtain access tokens, issued to the client by the authorization server and represented as a string. Refresh token can be used to obtain a new access token or to obtain additional access tokens with identical or narrower scope.

has super-classes
Token [C]

Resource Owner[C]

back to ToC or Class ToC

IRI: http://www.daspsec.org/o/oauth-2.0#ResourceOwner

An entity capable of granting access to a protected resource. When the resource owner is a person, it is referred to as an end-user.

has super-classes
thing [C]

Resource Server[C]

back to ToC or Class ToC

IRI: http://www.daspsec.org/o/oauth-2.0#ResourceServer

The server that hosts the protected resources, capable of accepting and responding to protected resource requests using access tokens.

has super-classes
thing [C]

Token[C]

back to ToC or Class ToC

IRI: http://www.daspsec.org/o/oauth-2.0#Token

Credential used to access the resource or perform an operation.

has super-classes
thing [C]
has sub-classes
Access Token [C], Refresh Token [C]

Token Endpoint[c]

back to ToC or Class ToC

IRI: http://www.daspsec.org/o/oauth-2.0#TokenEndpoint

An endpoint used by the client to exchange an authorization grant for an access token, typically with client authentication.

has super-classes
Endpoint [c]

4.2. Object Properties

hasEndpoint

hasEndpoint[op]

back to ToC or Object Property ToC

IRI: http://www.daspsec.org/o/oauth-2.0#hasEndpoint

Specifies the endpoint associated with the entity.

has super-properties
top object property
has range
Endpoint [c]

4.3. Data Properties

hasBearerTokenValue hasClientIdentifier hasClientPassword hasDesiredGrantType hasEndpointURI hasRefreshTokenValue hasTokenValue

hasBearerTokenValue[dp]

back to ToC or Data Property ToC

IRI: http://www.daspsec.org/o/oauth-2.0#hasBearerTokenValue

Specifies the value of OAuth 2.0 bearer token.

has super-properties
hasTokenValue [dp]
has domain
Client [c]
has range
string

hasClientIdentifier dp

back to ToC or Data Property ToC

IRI: http://www.daspsec.org/o/oauth-2.0#hasClientIdentifier

A unique string that represents registration information provided by the client at authorization server. The client identifier is not a secret; it is exposed to the resource owner and MUST NOT be used alone for client authentication. The client identifier is unique to the authorization server.

has super-properties
top data property

has domain
Client c

has range
string

hasClientPassword dp

back to ToC or Data Property ToC

IRI: http://www.daspsec.org/o/oauth-2.0#hasClientPassword

Client password used to authenticate at the autorization server.

has super-properties
top data property

has domain
Client c

has range
string

hasDesiredGrantType dp

back to ToC or Data Property ToC

IRI: http://www.daspsec.org/o/oauth-2.0#hasDesiredGrantType

Represents grant type requested from the authorization server. Grant type *code* is used to request authorization code, while grant type *token* is used to request an access token. Alternative type can be requested provided that it has been previously registered according to the specification.

has super-properties
top data property

has domain
Authorization Request c

has range
string

hasEndpointURI dp

back to ToC or Data Property ToC

IRI: http://www.daspsec.org/o/oauth-2.0#hasEndpointURI

References the endpoint URI used for interactions with the clients.

has super-properties
top data property

has range
any u r i

hasRefreshTokenValue dp

back to ToC or Data Property ToC

IRI: http://www.daspsec.org/o/oauth-2.0#hasRefreshTokenValue

Specifies the value of OAuth 2.0 refresh token.

has super-properties
hasTokenValue dp

has domain
Client c

has range
string

hasTokenValue dp

back to ToC or Data Property ToC

IRI: http://www.daspsec.org/o/oauth-2.0#hasTokenValue

Specifies the value of the provided token.

has super-properties
top data property

has sub-properties
hasBearerTokenValue dp, hasRefreshTokenValue dp

has domain
Client c **or** Token c

Legend

back to ToC

c: Classes
op: Object Properties
dp: Data Properties
ni: Named Individuals

5. References

back to ToC

[OAUTH2] RFC6749 - The OAuth 2.0 Authorization Framework. D. Hardt, Ed. (2012).
URL: https://tools.ietf.org/html/rfc6749

[XACML] eXtensible Access Control Markup Language (XACML) Version 3.0. OASIS standard, OASIS (2013).
URL: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html

[CSA] Cloud Security Open API Working Group: Proposed Charter. CSA Working Group (2015)
URL: https://cloudsecurityalliance.org/group/open-api/

[API16] Riding and thriving on the API hype cycle. Maja Vukovic et al. Communications of ACM 59, 3 (2016)
URL: https://cacm.acm.org/magazines/

[REST14] RESTful or RESTless – Current state of todays top Web APIs. Frederik Bülthoff and Maria Maleshkova. In European Semantic Web Conference. Springer (2014)
URL: http://rdcu.be/tM6B