RFC6750 - The OAuth 2.0 Authorization Framework: Bearer Token Usage

return to the IETF Standards

Table 1: The OAuth 2.0 Authorization Framework: Bearer Token Usage

Title	The OAuth 2.0 Authorization Framework: Bearer Token Usage
Acronym	TCP
Version	2.0
Document Number	RFC6750
Release Date	October 2012
Reference	https://tools.ietf.org/html/rfc6750

Note: The following is an excerpt from the official IETF RFC. It is provided here as a convenience and is not authoritative. Refer to the original document as the authoritative reference.

Introduction

OAuth enables clients to access protected resources by obtaining an access token, which is defined in "The OAuth 2.0 https://www.techopedia.com/definition/10237/authorization Framework" [RFC6749] as "a string representing an access authorization issued to the client", rather than using the resource owner's credentials directly.

Tokens are issued to clients by an authorization server with the approval of the resource owner. The client uses the access token to access the protected resources hosted by the resource server. This specification describes how to make protected resource requests when the OAuth access token is a bearer token.

This specification defines the use of bearer tokens over HTTP/1.1 RFC2616 using Transport Layer Security (TLS) RFC5246 to access protected resources. TLS is mandatory to implement and use with this specification; other specifications may extend this specification for use with other protocols. While designed for use with access tokens resulting from OAuth 2.0 authorization RFC6749 flows to access OAuth protected resources, this specification actually defines a general HTTP authorization method that can be used with bearer tokens from any source to access any resources protected by those bearer tokens. The Bearer authentication scheme is intended primarily for server authentication using the WWW-Authenticate and Authorization HTTP headers but does not preclude its use for proxy authentication.