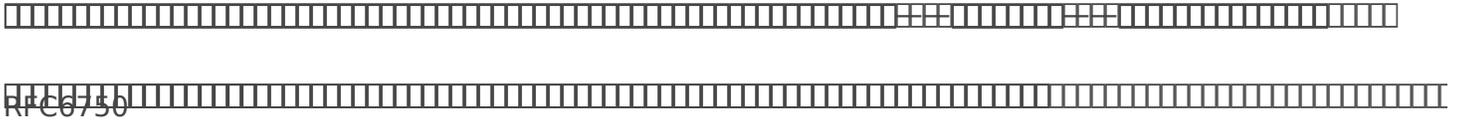


1.4. Access Token

1.4. Access Token



1.4. Access Token

Access tokens are credentials used to access protected resources. An access token is a string representing an authorization issued to the client. The string is usually opaque to the client. Tokens

represent specific scopes and durations of access, granted by the resource owner, and enforced by the resource server and authorization server.

The token may denote an identifier used to retrieve the authorization information or may self-contain the authorization information in a verifiable manner (i.e., a token string consisting of some data and a signature). Additional authentication credentials, which are beyond

the scope of this specification, may be required in order for the client to use a token.

The access token provides an abstraction layer, replacing different authorization constructs (e.g., username and password) with a single token understood by the resource server. This abstraction enables issuing access tokens more restrictive than the authorization grant

used to obtain them, as well as removing the resource server's need to understand a wide range of authentication methods.

Access tokens can have different formats, structures, and methods of utilization (e.g.,

cryptographic properties) based on the resource server security requirements. Access token attributes and the

methods used to access protected resources are beyond the scope of this specification and are defined by companion specifications such as [RFC6750].

Revision #2

Created Wed, Mar 25, 2020 12:17 AM by []

Updated Wed, Mar 25, 2020 12:22 AM by []