

# Lexicon

## Lexicon

### Terminology in the protocol spec

Following is a new proposal for OAuth 2.0-based terms, now incorporated into the core protocol spec. Key definitions from the draft OAuth 2.0 specification ([OAuth20]) are reproduced here for ease of tracing UMA definitions that are dependent on them, though these OAuth definitions do not appear in the formal spec.

**authorizing user:** An UMA-defined variant of an [OAuth20] resource owner (*"An entity capable of granting access to a protected resource."*); a web user who configures an authorization manager with policies that control how it makes access decisions when a requester attempts to access a protected resource at a host.

**authorization manager (AM):** An UMA-defined variant of an [OAuth20] authorization server (*"An HTTP server capable of issuing tokens after successfully authenticating the resource owner and obtaining authorization. The authorization server may be the same server as the resource server, or a separate entity."*) that carries out an authorizing user's policies governing access to a protected resource.

**protected resource:** An access-restricted resource at a host.

**host:** An UMA-defined variant of an [OAuth20] resource server (*"An HTTP server capable of accepting authenticated resource requests using the OAuth protocol."*) that enforces access to the protected resources it hosts, as decided by an authorization manager.

**token validation URL:** The URL at an authorization manager that a host can use to validate an access token.

**claim:** A statement (in the sense of [IDCclaim]). Claims are conveyed by a requester on behalf of a requesting party to an authorization manager in an attempt to satisfy an authorizing user's policy. (Protected resources may also contain claims, but this is outside the view of the UMA protocol.)

**requester:** An UMA-defined variant of [OAuth20] client (*"An HTTP client capable of making authenticated requests for protected resources using the OAuth protocol."*) that seeks access to a protected resource.

**requesting party:** A web user, or a corporation (or other legal person), that uses a requester to seek access to a protected resource.

### Additional terminology

Terms in this section do not appear in the protocol spec, but we have found it to be useful to define them in addition, for non-normative/discussion purposes.

**primary resource user:** A web user who who interacts with a host to store and manage protected resources there. The primary resource user may be identical to the authorizing user of the same resource at that host, or they they may be different people.

**UMAnitarian:** An UMA WG participant.

**UMAnize:** To make a host UMA-protected. (Thanks to Domenico for that one.)

### References

**[OAuth20]**

<http://github.com/theRazorBlade/draft-ietf-oauth/raw/master/draft-ietf-oauth.txt>

**[WRAP]**

<http://tools.ietf.org/html/draft-hardt-oauth-01>

**[hostmeta]**

<http://tools.ietf.org/html/draft-hammer-hostmeta>

**[IDCclaim]**

<http://wiki.idcommons.net/Claim>