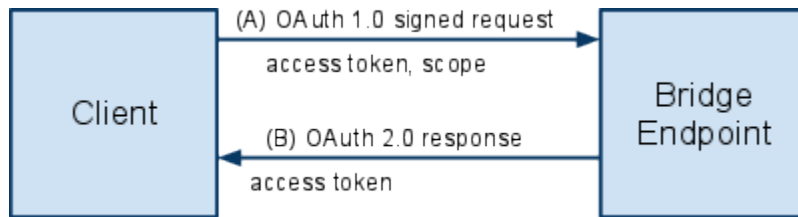# OAuth 1 Bridge

This flow defines an OAuth 1.0 to OAuth 2.0 bridge and it is implemented as an endpoint call. The bridge flow is suitable when the Client has an OAuth 1.0 access token and it wants to use OAuth 2.0 to access protected resources. The bridge endpoint allows the Client to exchange the OAuth 1.0 access token for a OAuth 2.0 access token.

The bridge flow illustrated above includes the following steps:
  * (A) The client makes an OAuth 1.0 signed request.
  * (B) The bridge endpoint validates the request and issue a short lived OAuth 2.0 access token.

1. Provisioning.

The Authorization Server must document the bridge endpoint URI.

2. Client calls the bridge endpoint.

The Client makes an OAuth 1.0 signed [RFC 5849, section 3] HTTP POST request to the bridge endpoint. The client constructs the request by adding the following parameters:
  * `scope` - OPTIONAL. Requested scope for the OAuth 2 access token. The specified scope must be a subset of the OAuth 1.0 access token scope.

The bridge endpoint MUST validate the OAuth 1.0 call and issue an OAuth 2.0 access token and deliver to the client in the HTTP response body using the `application/x-www-form-urlencoded` content type as defined by [W3C.REC-html40-19980424] with a 200 status code (OK).

The bridge endpoint MUST issue the OAuth 2.0 access token such that it grants access to the same protected resources as the incoming OAuth 1.0 access token. If the request specifies a `scope` paramter, then the bridge endpoint MUST verify that this scope grants access to a subset of the protected resources that can be accessed using the OAuth 1.0 access token.

The response contains the following parameters:
  * `access_token` - REQUIRED. The OAuth 2.0 access token.
  * `expires_in` - OPTIONAL. The duration in seconds of the access token lifetime.

If the request is invalid, the authorization server returns and error message in the HTTP response body using the `application/x-www-form-urlencoded` content type as defined by [W3C.REC-html40-19980424] with a 400 status code (Bad Request).

The response contains the following parameter:
- `error` - OPTIONAL. The parameter value MUST be set to one of: `"incorrect_credentials"`, `"invalid_scope"` or `"unauthorized_client"` (case sensitive).