Web Authorization Protocol
Internet-Draft
Updates: 8707 (if approved)
Intended status: Standards Track
Expires: 3 September 2026

F. Skokan
Okta

2 March 2026

Resource Indicator Response Parameter for OAuth 2.0
draft-skokan-oauth-resource-response-02

Abstract

This document defines the resource parameter for OAuth 2.0 access token responses, enabling an authorization server to indicate to the client the resource(s) which an issued access token is for. It updates "Resource Indicators for OAuth 2.0" (RFC 8707).

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://panva.github.io/draft-oauth-rfc8707bis/draft-skokan-oauth-resource-response.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-skokan-oauth-resource-response/.

Discussion of this document takes place on the Web Authorization Protocol Working Group mailing list (mailto:oauth@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/oauth/. Subscribe at https://www.ietf.org/mailman/listinfo/oauth/.

Source for this draft and an issue tracker can be found at https://github.com/panva/draft-oauth-rfc8707bis.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Copyright Notice

Table of Contents

1. Introduction

"Resource Indicators for OAuth 2.0" [RFC8707] defines the resource request parameter for use in authorization requests and access token requests, enabling a client to signal the target protected resource(s) to an authorization server. However, it does not define a corresponding response parameter that would allow the authorization server to communicate back to the client which resource(s) the issued access token is actually for.

Without a response parameter, a client cannot reliably determine the effective resource(s) of an issued access token when the authorization server restricts the token to a subset of the requested resources, or when it applies a default resource policy in cases where the client did not include the resource parameter in its request.

This document addresses that gap by defining the resource parameter for use in access token responses.

1.1. Requirements Notation and Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Access Token Response Resource Parameter

In access token responses, the resource parameter is represented as a JSON array of strings, unlike the repeated form-encoded or query parameter used in requests defined in [RFC8707].

The resource parameter defined for an access token response (Section 5.1 of [RFC6749]) is used to indicate to the client the resource(s) which an issued access token is for.

resource: OPTIONAL, if identical to the resource value(s) requested by the client; otherwise, REQUIRED. Its value is a JSON array of strings, where each string is an absolute URI as specified by Section 4.3 of [RFC3986], identifying a protected resource for which the access token is valid. The array MUST contain at least one value.

[[TODO: (#1 (https://github.com/panva/draft-oauth-rfc8707bis/issues/1)) Should the response use resource (a JSON string) when a single resource is indicated and resources (a JSON array of strings) when multiple are indicated instead?]]

The resource response parameter serves a similar role to the scope response parameter defined in Section 5.1 of [RFC6749]: it informs the client when the resource(s) associated with the issued access token differ from what the client requested. This can occur when the authorization server restricts the token to a subset of the requested resources, or when the authorization server applies a default resource policy in cases where the client did not include the resource parameter in its request.

If the client requested access to multiple resources but the authorization server issues an access token that is restricted to a subset of those resources, the authorization server MUST include the resource parameter in the response to inform the client of the effective resource(s). The client can then make additional token requests for the remaining resources as needed.

2.1. Scope or Policy Determined Resources

In some deployments, certain scope values are inherently associated with specific protected resources. For example, the openid scope in OpenID Connect [OpenID.Core] is tightly coupled to the UserInfo endpoint, and authorization servers may define scope values that are only meaningful at a particular resource.

When an authorization server issues an access token for a resource that it determined based on requested scope values or its own default policy, rather than from an explicit resource request parameter, the authorization server SHOULD use the resource's designated Resource Identifier [RFC9728] as the resource response parameter value. If no Resource Identifier is defined for the resource, the authorization server SHOULD use the exact URL of the protected resource instead. The value used SHOULD be one that the client can recognize and correlate with the intended protected resource (e.g., the UserInfo endpoint URL for an OpenID Provider when the openid scope is requested).

Since such a resource value was not explicitly requested by the client, the resource response parameter is REQUIRED in this case per the condition defined in Section 2.

The following is a non-normative example of a token endpoint response where the authorization server indicates that the issued access token is valid for use at https://cal.example.com/.

```
HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: no-cache, no-store

{
   "access_token": "_Q-oyRuYqHlj_ZgXwuS54thQm_L5GhB3XH20cVtYfq",
   "token_type": "Bearer",
   "expires_in":3600,
   "refresh_token": "4LTC8lb0acc6Oy4esc1Nk9BWC0imAwH7kic16BDC2",
   "scope": "calendar",
   "resource": ["https://cal.example.com/"]
}
```

Figure 1: Access Token Response with Resource

The following is a non-normative example of a token endpoint response where the authorization server, acting as an OpenID Provider, issues an access token for the UserInfo endpoint based on the openid scope value that was requested by the client. The authorization server uses the userinfo_endpoint URL from its discovery metadata as the resource value.

```
HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: no-cache, no-store

{
   "access_token": "_Q-oyRuYqHlj_ZgXwuS54thQm_L5GhB3XH2cVtYfqh",
   "token_type": "Bearer",
   "expires_in":3600,
   "refresh_token": "4LTC8lb0acc6Oy4esc1Nk9BWC0imAwH7kic16BDC2",
   "id_token": "eyJhbGciOiJSUzI...",
   "scope": "openid email profile",
   "resource": ["https://server.example.com/userinfo"]
}
```

Figure 2: Access Token Response with Scope-Determined Resource

3. Security Considerations

This document inherits the security considerations of [RFC8707].

Knowledge of the resource(s) for which an access token is valid does not introduce new security concerns for the client. The resource response parameter merely makes explicit information that the client either already requested or that the authorization server determined based on its policy.

4. Privacy Considerations

The resource response parameter conveys information about the resource(s) associated with an access token back to the client. Since the client either requested these resources or they were determined by authorization server policy, no new privacy-sensitive information is disclosed by this parameter.

5. IANA Considerations

5.1. OAuth Parameters Registration

This specification updates the following value in the IANA "OAuth Parameters" registry [IANA.OAuth.Parameters] established by [RFC6749].

Parameter name: resource
Parameter usage location: authorization request, token request, token response
Change controller: IETF
Specification document(s): Section 2 of [RFC8707] and Section 2 of this document

6. References

6.1. Normative References

[IANA.OAuth.Parameters]
IANA, "OAuth Parameters", <https://www.iana.org/assignments/oauth-parameters>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <https://www.rfc-editor.org/rfc/rfc3986>.

[RFC6749] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework", RFC 6749, DOI 10.17487/RFC6749, October 2012, <https://www.rfc-editor.org/rfc/rfc6749>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC8707] Campbell, B., Bradley, J., and H. Tschofenig, "Resource Indicators for OAuth 2.0", RFC 8707, DOI 10.17487/RFC8707, February 2020, <https://www.rfc-editor.org/rfc/rfc8707>.

6.2. Informative References

[OpenID.Core]
Sakimura, N., Bradley, J., Jones, M., Medeiros, B. de., and C. Mortimore, "OpenID Connect Core 1.0 incorporating

errata set 2", The OpenID Foundation , 15 December 2023, <https://openid.net/specs/openid-connect-core-1_0-errata2.html>.

[RFC9728] Jones, M.B., Hunt, P., and A. Parecki, "OAuth 2.0 Protected Resource Metadata", RFC 9728, DOI 10.17487/RFC9728, April 2025, <https://www.rfc-editor.org/rfc/rfc9728>.

Acknowledgments

The original "Resource Indicators for OAuth 2.0" specification [RFC8707] was authored by Brian Campbell, John Bradley, and Hannes Tschofenig.

Document History

draft-skokan-oauth-resource-response-02

* Added guidance on scope or policy determined resource values

draft-skokan-oauth-resource-response-01

draft-skokan-oauth-resource-response-00

* Initial draft defining the resource access token response parameter

Author’s Address

Filip Skokan
Okta
Email: panva.ip@gmail.com