International Standard

ISO/IEC 26139

First edition
2024-10

Information technology — OpenID connect — OAuth 2.0 form post response mode

Reference number
ISO/IEC 26139:2024(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by the OpenID Foundation (OIDF) (as OAuth 2.0 Form Post Response Mode) and drafted in accordance with its editorial rules. It was adopted, under the JTC 1 PAS procedure, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Abstract

This specification defines the Form Post Response Mode. In this mode, Authorization Response parameters are encoded as HTML form values that are auto-submitted in the User Agent, and thus are transmitted via the HTTP `POST` method to the Client, with the result parameters being encoded in the body using the `application/x-www-form-urlencoded` format.

Table of Contents

Information technology — OpenID Connect — OAuth 2.0 Form Post Response Mode

1. Introduction

TOC

1.1. Requirements Notation and Conventions

TOC

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

In the .txt version of this document, values are quoted to indicate that they are to be taken literally. When using these values in protocol messages, the quotes MUST NOT be used as part of the value. In the HTML version of this document, values to be taken literally are indicated by the use of `this fixed-width font`.

1.2. Terminology

TOC

This specification uses the terms "Access Token", "Authorization Code", "Authorization Endpoint", "Authorization Grant", "Authorization Server", "Client", "Client Identifier", "Client Secret", "Protected Resource", "Redirection URI", "Refresh Token", "Resource Owner", "Resource Server", "Response Type", and "Token Endpoint" defined by OAuth 2.0 [RFC6749] the term "User Agent" defined by RFC 7230 [RFC7230], and the term "Response Mode" defined by OAuth 2.0 Multiple Response Type Encoding Practices [OAuth.Responses].

2. Form Post Response Mode

TOC

This specification defines the Form Post Response Mode, which is described with its `response_mode` parameter value:

form_post

In this mode, Authorization Response parameters are encoded as HTML form values that are auto-submitted in the User Agent, and thus are transmitted via the HTTP `POST` method to the Client, with the result parameters being encoded in the body using the `application/x-www-form-urlencoded` format. The action attribute of the form MUST be the Client's Redirection URI. The method of the form attribute MUST be `POST`. Because the Authorization Response is intended to be used only once, the Authorization Server MUST instruct the User Agent (and any intermediaries) not to store or reuse the content of the response.

Any technique supported by the User Agent MAY be used to cause the submission of the form, and any form content necessary to support this MAY be included, such as submit controls and client-side scripting commands. However, the Client MUST be able to process the message without regard for the mechanism by which the form submission was initiated.

---

3. IANA Considerations

TOC

This specification makes no requests of IANA.

---

4. Security Considerations

TOC

As described in OAuth 2.0 Multiple Response Type Encoding Practices [OAuth.Responses], there are security implications to encoding response values in the query string and in the fragment value. Some of these concerns can be addressed by using the Form Post Response Mode. In particular, it is safe to return Authorization Response parameters whose default Response Modes are the query encoding or the fragment encoding using the `form_post` Response Mode.

5. Normative References

TOC

[OAuth.Responses] de Medeiros, B., Ed., Scurtescu, M., Tarjan, P., and M. Jones, "OAuth 2.0 Multiple Response Type Encoding Practices," February 2014.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).

[RFC6749] Hardt, D., "The OAuth 2.0 Authorization Framework," RFC 6749, October 2012 (TXT).

[RFC7230] Fielding, R. and J. Reschke, "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing," RFC 7230, June 2014 (TXT).

Appendix A. "form_post" Response Mode Example

TOC

Below is a non-normative request/response/request example as issued/received/issued by the User Agent (with extra line breaks for display purposes only) demonstrating an auto-submitted `form_post` encoded response.

Authorization Request to the Authorization Endpoint:

```
GET /authorize?
 response_type=id_token
 &response_mode=form_post
 &client_id=some_client
 &scope=openid
 &redirect_uri=https%3A%2F%2Fclient.example.org%2Fcallback
 &state=DcP7csa3hMlvybERqcieLHrRzKBra
 &nonce=2T1AgaeRTGTMAJyeDMN9IJbgiUG HTTP/1.1
Host: server.example.com
```

After authentication and approval by the End-User, the Authorization Server issues the Authorization Response:

```
HTTP/1.1 200 OK
Content-Type: text/html;charset=UTF-8
Cache-Control: no-cache, no-store
Pragma: no-cache
```