|  |
| --- |
| **[TOC](" \l "toc)** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | Draft | M. Jones | |  | Microsoft | |  | B. Campbell | |  | Ping Identity | |  | March 5, 2015 | |

# OAuth 2.0 Form Post Response Mode - draft 04

### 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

[**1.**](#Introduction)  Introduction  
    [**1.1.**](#rnc)  Requirements Notation and Conventions  
    [**1.2.**](#Terminology)  Terminology  
[**2.**](#FormPostResponseMode)  Form Post Response Mode  
[**3.**](#IANA)  IANA Considerations  
[**4.**](#Security)  Security Considerations  
[**5.**](#rfc.references1)  Normative References  
[**Appendix A.**](#FormPostResponseExample)  "form\_post" Response Mode Example  
[**Appendix B.**](#Acknowledgements)  Acknowledgements  
[**Appendix C.**](#Notices)  Notices  
[**Appendix D.**](#History)  Document History  
[**§**](#rfc.authors)  Authors' Addresses

|  |
| --- |
| [**TOC**](#toc) |

### 1.  Introduction

|  |
| --- |
| [**TOC**](#toc) |

### 1.1.  Requirements Notation and Conventions

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 (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.)](#RFC2119) [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.

|  |
| --- |
| [**TOC**](#toc) |

### 1.2.  Terminology

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 (Hardt, D., “The OAuth 2.0 Authorization Framework,” October 2012.)](#RFC6749) [RFC6749] the term "User Agent" defined by [RFC 7230 (Fielding, R. and J. Reschke, “Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing,” June 2014.)](" \l "RFC7230) [RFC7230], and the term "Response Mode" defined by [OAuth 2.0 Multiple Response Type Encoding Practices (de Medeiros, B., Ed., Scurtescu, M., Tarjan, P., and M. Jones, “OAuth 2.0 Multiple Response Type Encoding Practices,” February 2014.)](#OAuth.Responses) [OAuth.Responses].

|  |
| --- |
| [**TOC**](#toc) |

### 2.  Form Post Response Mode

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.

|  |
| --- |
| [**TOC**](#toc) |

### 3.  IANA Considerations

This specification makes no requests of IANA.

|  |
| --- |
| [**TOC**](#toc) |

### 4.  Security Considerations

As described in [OAuth 2.0 Multiple Response Type Encoding Practices (de Medeiros, B., Ed., Scurtescu, M., Tarjan, P., and M. Jones, “OAuth 2.0 Multiple Response Type Encoding Practices,” February 2014.)](#OAuth.Responses) [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.

|  |
| --- |
| [**TOC**](#toc) |

### 5. Normative References

|  |  |
| --- | --- |
| **[OAuth.Responses]** | de Medeiros, B., Ed., Scurtescu, M., Tarjan, P., and M. Jones, “[OAuth 2.0 Multiple Response Type Encoding Practices](http://openid.net/specs/oauth-v2-multiple-response-types-1_0.html),” February 2014. |
| **[RFC2119]** | [Bradner, S.](mailto:sob@harvard.edu), “[Key words for use in RFCs to Indicate Requirement Levels](http://tools.ietf.org/html/rfc2119),” BCP 14, RFC 2119, March 1997 ([TXT](http://www.rfc-editor.org/rfc/rfc2119.txt), [HTML](http://xml.resource.org/public/rfc/html/rfc2119.html), [XML](http://xml.resource.org/public/rfc/xml/rfc2119.xml)). |



|  |  |
| --- | --- |
| **[RFC6749]** | Hardt, D., “[The OAuth 2.0 Authorization Framework](http://tools.ietf.org/html/rfc6749),” RFC 6749, October 2012 ([TXT](http://www.rfc-editor.org/rfc/rfc6749.txt)). |
| **[RFC7230]** | Fielding, R. and J. Reschke, “[Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing](http://tools.ietf.org/html/rfc7230),” RFC 7230, June 2014 ([TXT](http://www.rfc-editor.org/rfc/rfc7230.txt)). |

|  |
| --- |
| [**TOC**](#toc) |

### Appendix A.  "form\_post" Response Mode Example

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

<html>

<head><title>Submit This Form</title></head>

<body onload="javascript:document.forms[0].submit()">

<form method="post" action="https://client.example.org/callback">

<input type="hidden" name="state"

value="DcP7csa3hMlvybERqcieLHrRzKBra"/>

<input type="hidden" name="id\_token"

value="eyJhbGciOiJSUzI1NiIsImtpZCI6IjEifQ.eyJzdWIiOiJqb2huIiw

iYXVkIjoiZmZzMiIsImp0aSI6ImhwQUI3RDBNbEo0c2YzVFR2cllxUkIiLC

Jpc3MiOiJodHRwczpcL1wvbG9jYWxob3N0OjkwMzEiLCJpYXQiOjEzNjM5M

DMxMTMsImV4cCI6MTM2MzkwMzcxMywibm9uY2UiOiIyVDFBZ2FlUlRHVE1B

SnllRE1OOUlKYmdpVUciLCJhY3IiOiJ1cm46b2FzaXM6bmFtZXM6dGM6U0F

NTDoyLjA6YWM6Y2xhc3NlczpQYXNzd29yZCIsImF1dGhfdGltZSI6MTM2Mz

kwMDg5NH0.c9emvFayy-YJnO0kxUNQqeAoYu7sjlyulRSNrru1ySZs2qwqq

wwq-Qk7LFd3iGYeUWrfjZkmyXeKKs\_OtZ2tI2QQqJpcfrpAuiNuEHII-\_fk

IufbGNT\_rfHUcY3tGGKxcvZO9uvgKgX9Vs1v04UaCOUfxRjSVlumE6fWGcq

XVEKhtPadj1elk3r4zkoNt9vjUQt9NGdm1OvaZ2ONprCErBbXf1eJb4NW\_h

nrQ5IKXuNsQ1g9ccT5DMtZSwgDFwsHMDWMPFGax5Lw6ogjwJ4AQDrhzNCFc

0uVAwBBb772-86HpAkGWAKOK-wTC6ErRTcESRdNRe0iKb47XRXaoz5acA"/>

</form>

</body>

</html>

which results in an HTTP POST to the Client:

POST /callback HTTP/1.1

Host: client.example.org

Content-Type: application/x-www-form-urlencoded

id\_token=eyJhbGciOiJSUzI1NiIsImtpZCI6IjEifQ.eyJzdWIiOiJqb2huIiwiYX

VkIjoiZmZzMiIsImp0aSI6ImhwQUI3RDBNbEo0c2YzVFR2cllxUkIiLCJpc

3MiOiJodHRwczpcL1wvbG9jYWxob3N0OjkwMzEiLCJpYXQiOjEzNjM5MDMx

MTMsImV4cCI6MTM2MzkwMzcxMywibm9uY2UiOiIyVDFBZ2FlUlRHVE1BSnl

lRE1OOUlKYmdpVUciLCJhY3IiOiJ1cm46b2FzaXM6bmFtZXM6dGM6U0FNTD

oyLjA6YWM6Y2xhc3NlczpQYXNzd29yZCIsImF1dGhfdGltZSI6MTM2MzkwM

Dg5NH0.c9emvFayy-YJnO0kxUNQqeAoYu7sjlyulRSNrru1ySZs2qwqqwwq

-Qk7LFd3iGYeUWrfjZkmyXeKKs\_OtZ2tI2QQqJpcfrpAuiNuEHII-\_fkIuf

bGNT\_rfHUcY3tGGKxcvZO9uvgKgX9Vs1v04UaCOUfxRjSVlumE6fWGcqXVE

KhtPadj1elk3r4zkoNt9vjUQt9NGdm1OvaZ2ONprCErBbXf1eJb4NW\_hnrQ

5IKXuNsQ1g9ccT5DMtZSwgDFwsHMDWMPFGax5Lw6ogjwJ4AQDrhzNCFc0uV

AwBBb772-86HpAkGWAKOK-wTC6ErRTcESRdNRe0iKb47XRXaoz5acA&

state=DcP7csa3hMlvybERqcieLHrRzKBra

|  |
| --- |
| [**TOC**](#toc) |

### Appendix B.  Acknowledgements

The OpenID Community would like to thank the following people for their contributions to this specification:

Brian Campbell (bcampbell@pingidentity.com), Ping Identity

Michael B. Jones (mbj@microsoft.com), Microsoft

Breno de Medeiros (breno@google.com), Google

|  |
| --- |
| [**TOC**](#toc) |

### Appendix C.  Notices

Copyright (c) 2015 The OpenID Foundation.

The OpenID Foundation (OIDF) grants to any Contributor, developer, implementer, or other interested party a non-exclusive, royalty free, worldwide copyright license to reproduce, prepare derivative works from, distribute, perform and display, this Implementers Draft or Final Specification solely for the purposes of (i) developing specifications, and (ii) implementing Implementers Drafts and Final Specifications based on such documents, provided that attribution be made to the OIDF as the source of the material, but that such attribution does not indicate an endorsement by the OIDF.

The technology described in this specification was made available from contributions from various sources, including members of the OpenID Foundation and others. Although the OpenID Foundation has taken steps to help ensure that the technology is available for distribution, it takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this specification or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any independent effort to identify any such rights. The OpenID Foundation and the contributors to this specification make no (and hereby expressly disclaim any) warranties (express, implied, or otherwise), including implied warranties of merchantability, non-infringement, fitness for a particular purpose, or title, related to this specification, and the entire risk as to implementing this specification is assumed by the implementer. The OpenID Intellectual Property Rights policy requires contributors to offer a patent promise not to assert certain patent claims against other contributors and against implementers. The OpenID Foundation invites any interested party to bring to its attention any copyrights, patents, patent applications, or other proprietary rights that may cover technology that may be required to practice this specification.

|  |
| --- |
| [**TOC**](#toc) |

### Appendix D.  Document History

[[ To be removed from the final specification ]]

-04

* Added normative language about not caching responses and updated the example Cache-Control directive.
* Updated the RFC 2616 reference to RFC 7230.

-03

* Updated dates for final OpenID Connect specifications.

-02

* Applied review comments by Brian Campbell.

-01

* Created the initial draft by extracting the form\_post Response Mode definition from the OAuth 2.0 Multiple Response Type Encoding Practices specification.

|  |
| --- |
| [**TOC**](#toc) |

### Authors' Addresses

|  |  |
| --- | --- |
|  | Michael B. Jones |
|  | Microsoft |
| **Email:** | [mbj@microsoft.com](mailto:mbj@microsoft.com) |
| **URI:** | <http://self-issued.info/> |
|  |  |
|  | Brian Campbell |
|  | Ping Identity |
| **Email:** | [brian.d.campbell@gmail.com](mailto:brian.d.campbell@gmail.com) |
| **URI:** | <https://twitter.com/__b_c> |