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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | Draft | N. Sakimura | |  | NRI | |  | J. Bradley, Ed. | |  | Protiviti | |  | M. Jones | |  | Microsoft | |  | September 30, 2011 | |

# OpenID Connect Dynamic Client Registration 1.0 - draft 07

### Abstract

OpenID Connect is an identity protocol that provides authentication, authorization, and attribute transmission capability. It allows third party attested claims from distributed sources. The specification suite builds on OAuth 2.0 and consists of Building Blocks (Messages, Discovery, Dynamic Client Registration, Session Management, JSON Web Token, JSON Web Signature, JSON WEB Encryption, JSON Web Keys, Simple Web Discovery), Protocol Bindings (e.g., Standard and Basic Client) and Extensions. This specification is the "Dynamic Client Registration" part of the suite that defines how clients register with OpenID Providers.

### Requirements Language

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].

### Table of Contents

[**1.**](#anchor1)  Introduction  
[**2.**](#terminology)  Terminology  
[**3.**](#anchor2)  Discovery  
[**4.**](#anchor3)  Client Registration Endpoint  
    [**4.1.**](#anchor4)  Request  
    [**4.2.**](#anchor5)  Response  
[**5.**](#IANA)  IANA Considerations  
[**6.**](#Security)  Security Considerations  
[**7.**](#rfc.references1)  Normative References  
[**Appendix A.**](#Acknowledgements)  Acknowledgements  
[**Appendix B.**](#anchor7)  Document History  
[**§**](#rfc.authors)  Authors' Addresses

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

### 1.  Introduction

In order for an OpenID Connect client to utilize OpenID services for a user, the client needs to register with the OpenID Provider to acquire a client ID and shared secret. This document describes how a new client can register with the provider, and how a client already in possession of a client\_id can retrieve updated registration information.

The Client Registration endpoint may be co-resident with the token endpoint as an optimization in some deployments.

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

### 2.  Terminology

This specification uses the terms "Access Token", "Refresh Token", "Authorization Code", "Authorization Grant", "Authorization Server", "Authorization Endpoint", "Client", "Client Identifier", "Client Secret", "Protected Resource", "Resource Owner", "Resource Server", and "Token Endpoint" that are defined by [OAuth 2.0 (Hammer-Lahav, E., Ed., Recordon, D., and D. Hardt, “OAuth 2.0 Authorization Protocol,” September 2011.)](#OAuth.2.0) [OAuth.2.0], and the terminology defined in the [OpenID Connect Messages 1.0 (Sakimura, N., Recordon, D., Bradley, J., de Medeiros, B., Jones, M., and E. Jay, “OpenID Connect Messages 1.0,” September 2011.)](#OpenID.Messages) [OpenID.Messages] specification.

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

### 3.  Discovery

OpenID Connect uses the registration\_endpoint from the Provider Configuration Response [Sec 4.2 (Sakimura, N., Bradley, J., Jones, M., and E. Jay, “OpenID Connect Discovery 1.0,” September 2011.)](#OpenID.Discovery) [OpenID.Discovery].

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

### 4.  Client Registration Endpoint

The Client Registration Endpoint returns registration information for the client to configure itself for the OpenID Provider.

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

### 4.1.  Request

Clients MUST send requests encoded as a POST with the following parameters added to the HTTP request entity-body using "application/x-www-form-urlencoded" format:

type

REQUIRED. Values client\_associate, client\_update

client\_id

OPTIONAL. Used with client\_update

client\_secret

OPTIONAL. Used with client\_update

contact

OPTIONAL. Space-separated of e-mail addresses for people allowed toadminister the application.

application\_type

OPTIONAL. native or web.

application\_name

OPTIONAL. Name of the application to be presented to the user.

logo\_url

OPTIONAL. URL that a logo for the application can be retrieved from.

redirect\_uri

OPTIONAL. Space-separated list of redirect URIs

js\_origin\_uri

OPTIONAL. Space-separated list of JavaScript Origin URIs (used for Post Message flow)

jwk\_url

OPTIONAL. URL for the RP's [JSON Web Key (Jones, M., “JSON Web Key (JWK),” July 2011.)](#JWK) [JWK]

x509\_url

OPTIONAL URL for the RP's PEM encoded X.509 Certificate or Certificate chain.

sector\_identifier

OPTIONAL URL to be used in calculating Pseudonymous Identifiers by the OP. The URL contains a file with an array of redirect\_uri values.

POST /connect/register HTTP/1.1

Accept: application/x-www-form-urlencoded

Host: server.example.com

type=client\_associate

&redirect\_uri=https://client.example.com/callback https://client.example.com/callback2

&logo\_url=https://client.example.com/logo.png

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

### 4.2.  Response

The response is returned as a JSON object with all the parameters as top level elements.

client\_id

REQUIRED. The unique client identifier.

client\_secret

REQUIRED. The client secret. This should change with each response.

expires\_in

REQUIRED. The number of seconds that this id and secret are good for or 0 if it does not expire.

The following is an example response.

HTTP/1.1 200 OK

Content-Type: application/json

Cache-Control: no-store

{

"client\_id":"SlAV32hkKG",

"client\_secret":"cf136dc3c1fd9153029bb9c6cc9ecead918bad9887fce6c93f31185e5885805d",

"expires\_in":3600

}

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

### 5.  IANA Considerations

This document makes no request of IANA.

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

### 6.  Security Considerations

Since requests to the client registration endpoint result in the transmission of clear-text credentials (in the HTTP request and response), the server MUST require the use of a transport-layer security mechanism when sending requests to the token endpoint. The server MUST support TLS 1.2 as defined in [RFC5246], and MAY support additional transport-layer mechanisms meeting its security requirements.

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

### 7. Normative References

|  |  |
| --- | --- |
| **[JWK]** | Jones, M., “[JSON Web Key (JWK)](http://self-issued.info/docs/draft-jones-json-web-key.html),” July 2011. |
| **[OAuth.2.0]** | Hammer-Lahav, E., Ed., Recordon, D., and D. Hardt, “[OAuth 2.0 Authorization Protocol](http://tools.ietf.org/html/draft-ietf-oauth-v2),” September 2011. |
| **[OpenID.Discovery]** | Sakimura, N., Bradley, J., Jones, M., and E. Jay, “[OpenID Connect Discovery 1.0](http://openid.net/specs/openid-connect-discovery-1_0.html),” September 2011. |
| **[OpenID.Messages]** | Sakimura, N., Recordon, D., Bradley, J., de Medeiros, B., Jones, M., and E. Jay, “[OpenID Connect Messages 1.0](http://openid.net/specs/openid-connect-messages-1_0.html),” September 2011. |
| **[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)). |

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

### Appendix A.  Acknowledgements

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

### Appendix B.  Document History

[[ To be removed from the final specification ]]

-07

* Changed request from posting a JSON object to being HTTP Form encoded.
* Added x509\_url to support optional encryption.

-06

* Changes associated with renaming "Lite" to "Basic Client" and replacing "Core" and "Framework" with "Messages" and "Standard".
* Numerous cleanups, including updating references.

-05

* Changed redirect\_url to redirect\_uri and js\_origin\_url to js\_origin\_uri.

-04

* Correct issues raised by Johnny Bufu and discussed on the 7-Jul-11 working group call.

-03

* Incorporate working group decisions from 5-Jul-11 spec call.
* Consistency and cleanup pass, including removing unused references.

-02

* Incorporate working group decisions from 23-Jun-11 spec call.

-01

* Initial version.

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

### Authors' Addresses

|  |  |
| --- | --- |
|  | Nat Sakimura |
|  | Nomura Research Institute, Ltd. |
| **Email:** | [n-sakimura@nri.co.jp](mailto:n-sakimura@nri.co.jp) |
|  |  |
|  | John Bradley (editor) |
|  | Protiviti Government Services |
| **Email:** | [jbradley@mac.com](mailto:jbradley@mac.com) |
|  |  |
|  | Michael B. Jones |
|  | Microsoft Corporation |
| **Email:** | [mbj@microsoft.com](mailto:mbj@microsoft.com) |