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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | Draft | N. Sakimura | |  | NRI | |  | J. Bradley | |  | Ping Identity | |  | M. Jones | |  | Microsoft | |  | August 3, 2015 | |

# OpenID Connect Dynamic Client Registration 1.0 - draft 29 incorporating errata set 2

### Abstract

OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. It enables Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner.

This specification defines how an OpenID Connect Relying Party can dynamically register with the End-User's OpenID Provider, providing information about itself to the OpenID Provider, and obtaining information needed to use it, including the OAuth 2.0 Client ID for this Relying Party.

### Table of Contents

[**1.**](#Introduction)  Introduction  
    [**1.1.**](#rnc)  Requirements Notation and Conventions  
    [**1.2.**](#Terminology)  Terminology  
[**2.**](#ClientMetadata)  Client Metadata  
    [**2.1.**](#LanguagesAndScripts)  Metadata Languages and Scripts  
[**3.**](#ClientRegistration)  Client Registration Endpoint  
    [**3.1.**](#RegistrationRequest)  Client Registration Request  
    [**3.2.**](#RegistrationResponse)  Client Registration Response  
    [**3.3.**](#RegistrationError)  Client Registration Error Response  
[**4.**](#ClientConfigurationEndpoint)  Client Configuration Endpoint  
    [**4.1.**](#AccessURL)  Forming the Client Configuration Endpoint URL  
    [**4.2.**](#ReadRequest)  Client Read Request  
    [**4.3.**](#ReadResponse)  Client Read Response  
    [**4.4.**](#ReadError)  Client Read Error Response  
[**5.**](#SectorIdentifierValidation)  "sector\_identifier\_uri" Validation  
[**6.**](#StringOps)  String Operations  
[**7.**](#Validation)  Validation  
[**8.**](#ImplementationConsiderations)  Implementation Considerations  
    **[8.1.](" \l "CompatibilityNotes)**  Compatibility Notes  
    [**8.2.**](#StatelessRegistration)  Implementation Notes on Stateless Dynamic Client Registration  
[**9.**](#Security)  Security Considerations  
    [**9.1.**](#Impersonation)  Impersonation  
    [**9.2.**](#NativeCodeLeakage)  Native Code Leakage  
    [**9.3.**](#TLSRequirements)  TLS Requirements  
[**10.**](#IANA)  IANA Considerations  
    **[10.1.](" \l "DynRegRegistrations)**  OAuth Dynamic Client Registration Metadata Registration  
        **[10.1.1.](" \l "DynRegContents)**  Registry Contents  
    **[10.2.](" \l "TEAMRegistration)**  OAuth Token Endpoint Authentication Methods Registration  
        **[10.2.1.](" \l "TEAMContents)**  Registry Contents  
[**11.**](#rfc.references1)  References  
    [**11.1.**](#rfc.references1)  Normative References  
    [**11.2.**](#rfc.references2)  Informative References  
[**Appendix A.**](#Acknowledgements)  Acknowledgements  
[**Appendix B.**](#Notices)  Notices  
**[Appendix C.](" \l "History)**  Document History  
[**§**](#rfc.authors)  Authors' Addresses

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

### 1.  Introduction

OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 [[RFC6749] (Hardt, D., Ed., “The OAuth 2.0 Authorization Framework,” October 2012.)](" \l "RFC6749) protocol. It enables Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner.

In order for an OpenID Connect Relying Party to utilize OpenID Connect services for an End-User, the RP needs to register with the OpenID Provider to provide the OP information about itself and to obtain information needed to use it, including an OAuth 2.0 Client ID. This document describes how an RP can register with an OP, and how registration information for the RP can be retrieved.

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

### 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 [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.

All uses of [JSON Web Signature (JWS) (Jones, M., Bradley, J., and N. Sakimura, “JSON Web Signature (JWS),” May 2015.)](" \l "JWS) [JWS] and [JSON Web Encryption (JWE) (Jones, M., Rescorla, E., and J. Hildebrand, “JSON Web Encryption (JWE),” May 2015.)](" \l "JWE) [JWE] data structures in this specification utilize the JWS Compact Serialization or the JWE Compact Serialization; the JWS JSON Serialization and the JWE JSON Serialization are not used.

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

### 1.2.  Terminology

This specification uses the terms "Access Token", "Authorization Code", "Authorization Endpoint", "Authorization Grant", "Authorization Server", "Client", "Client Authentication", "Client Identifier", "Client Secret", "Grant Type", "Protected Resource", "Redirection URI", "Refresh Token", "Resource Owner", "Resource Server", "Response Type", and "Token Endpoint" defined by [OAuth 2.0 (Hardt, D., Ed., “The OAuth 2.0 Authorization Framework,” October 2012.)](" \l "RFC6749) [RFC6749], the terms "JSON Web Token (JWT)" and "Nested JWT" defined by [JSON Web Token (JWT) (Jones, M., Bradley, J., and N. Sakimura, “JSON Web Token (JWT),” May 2015.)](" \l "JWT) [JWT], and the terms defined by [OpenID Connect Core 1.0 (Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and C. Mortimore, “OpenID Connect Core 1.0,” August 2015.)](" \l "OpenID.Core) [OpenID.Core].

This specification defines the following additional terms:

Client Registration Endpoint

OAuth 2.0 Protected Resource through which a Client can be registered at an Authorization Server.

Client Configuration Endpoint

OAuth 2.0 Endpoint through which registration information for a registered Client can be managed. This URL for this endpoint is returned by the Authorization Server in the Client Information Response.

Registration Access Token

OAuth 2.0 Bearer Token issued by the Authorization Server through the Client Registration Endpoint that is used to authenticate the caller when accessing the Client's registration information at the Client Configuration Endpoint. This Access Token is associated with a particular registered Client.

Initial Access Token

OAuth 2.0 Access Token optionally issued by an Authorization Server granting access to its Client Registration Endpoint. The contents of this token are service specific and are out of scope for this specification. The means by which the Authorization Server issues this token and the means by which the Registration Endpoint validates it are also out of scope.

IMPORTANT NOTE TO READERS: The terminology definitions in this section are a normative portion of this specification, imposing requirements upon implementations. All the capitalized words in the text of this specification, such as "Client Registration Endpoint", reference these defined terms. Whenever the reader encounters them, their definitions found in this section must be followed.

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

### 2.  Client Metadata

Clients have metadata associated with their unique Client Identifier at the Authorization Server. These can range from human-facing display strings, such as a Client name, to items that impact the security of the protocol, such as the list of valid redirect URIs.

The Client Metadata values are used in two ways:

* as input values to registration requests, and
* as output values in registration responses and read responses.

These Client Metadata values are used by OpenID Connect:

redirect\_uris

REQUIRED. Array of Redirection URI values used by the Client. One of these registered Redirection URI values MUST exactly match the redirect\_uri parameter value used in each Authorization Request, with the matching performed as described in Section 6.2.1 of [[RFC3986] (Berners-Lee, T., Fielding, R., and L. Masinter, “Uniform Resource Identifier (URI): Generic Syntax,” January 2005.)](#RFC3986) (Simple String Comparison).

response\_types

OPTIONAL. JSON [[RFC7159] (Bray, T., Ed., “The JavaScript Object Notation (JSON) Data Interchange Format,” March 2014.)](" \l "RFC7159) array containing a list of the OAuth 2.0 response\_type values that the Client is declaring that it will restrict itself to using. If omitted, the default is that the Client will use only the code Response Type.

grant\_types

OPTIONAL. JSON array containing a list of the OAuth 2.0 Grant Types that the Client is declaring that it will restrict itself to using. The Grant Type values used by OpenID Connect are:

* authorization\_code: The Authorization Code Grant Type described in OAuth 2.0 Section 4.1.
* implicit: The Implicit Grant Type described in OAuth 2.0 Section 4.2.
* refresh\_token: The Refresh Token Grant Type described in OAuth 2.0 Section 6.

The following table lists the correspondence between response\_type values that the Client will use and grant\_type values that MUST be included in the registered grant\_types list:

* code: authorization\_code
* id\_token: implicit
* token id\_token: implicit
* code id\_token: authorization\_code, implicit
* code token: authorization\_code, implicit
* code token id\_token: authorization\_code, implicit

If omitted, the default is that the Client will use only the authorization\_code Grant Type.

application\_type

OPTIONAL. Kind of the application. The default, if omitted, is web. The defined values are native or web. Web Clients using the OAuth Implicit Grant Type MUST only register URLs using the https scheme as redirect\_uris; they MUST NOT use localhost as the hostname. Native Clients MUST only register redirect\_uris using custom URI schemes or URLs using the http: scheme with localhost as the hostname. Authorization Servers MAY place additional constraints on Native Clients. Authorization Servers MAY reject Redirection URI values using the http scheme, other than the localhost case for Native Clients. The Authorization Server MUST verify that all the registered redirect\_uris conform to these constraints. This prevents sharing a Client ID across different types of Clients.

contacts

OPTIONAL. Array of e-mail addresses of people responsible for this Client. This might be used by some providers to enable a Web user interface to modify the Client information.

client\_name

OPTIONAL. Name of the Client to be presented to the End-User. If desired, representation of this Claim in different languages and scripts is represented as described in [Section 2.1 (Metadata Languages and Scripts)](#LanguagesAndScripts).

logo\_uri

OPTIONAL. URL that references a logo for the Client application. If present, the server SHOULD display this image to the End-User during approval. The value of this field MUST point to a valid image file. If desired, representation of this Claim in different languages and scripts is represented as described in [Section 2.1 (Metadata Languages and Scripts)](#LanguagesAndScripts).

client\_uri

OPTIONAL. URL of the home page of the Client. The value of this field MUST point to a valid Web page. If present, the server SHOULD display this URL to the End-User in a followable fashion. If desired, representation of this Claim in different languages and scripts is represented as described in [Section 2.1 (Metadata Languages and Scripts)](#LanguagesAndScripts).

policy\_uri

OPTIONAL. URL that the Relying Party Client provides to the End-User to read about the how the profile data will be used. The value of this field MUST point to a valid web page. The OpenID Provider SHOULD display this URL to the End-User if it is given. If desired, representation of this Claim in different languages and scripts is represented as described in [Section 2.1 (Metadata Languages and Scripts)](#LanguagesAndScripts).

tos\_uri

OPTIONAL. URL that the Relying Party Client provides to the End-User to read about the Relying Party's terms of service. The value of this field MUST point to a valid web page. The OpenID Provider SHOULD display this URL to the End-User if it is given. If desired, representation of this Claim in different languages and scripts is represented as described in [Section 2.1 (Metadata Languages and Scripts)](#LanguagesAndScripts).

jwks\_uri

OPTIONAL. URL for the Client's JWK Set [[JWK] (Jones, M., “JSON Web Key (JWK),” May 2015.)](" \l "JWK) document. If the Client signs requests to the Server, it contains the signing key(s) the Server uses to validate signatures from the Client. The JWK Set MAY also contain the Client's encryption keys(s), which are used by the Server to encrypt responses to the Client. When both signing and encryption keys are made available, a use (public key use) parameter value is REQUIRED for all keys in the referenced JWK Set to indicate each key's intended usage. Although some algorithms allow the same key to be used for both signatures and encryption, doing so is NOT RECOMMENDED, as it is less secure. The JWK x5c parameter MAY be used to provide X.509 representations of keys provided. When used, the bare key values MUST still be present and MUST match those in the certificate.

jwks

OPTIONAL. Client's JWK Set [[JWK] (Jones, M., “JSON Web Key (JWK),” May 2015.)](" \l "JWK) document, passed by value. The semantics of the jwks parameter are the same as the jwks\_uri parameter, other than that the JWK Set is passed by value, rather than by reference. This parameter is intended only to be used by Clients that, for some reason, are unable to use the jwks\_uri parameter, for instance, by native applications that might not have a location to host the contents of the JWK Set. If a Client can use jwks\_uri, it MUST NOT use jwks. One significant downside of jwks is that it does not enable key rotation (which jwks\_uri does, as described in Section 10 of [OpenID Connect Core 1.0 (Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and C. Mortimore, “OpenID Connect Core 1.0,” August 2015.)](" \l "OpenID.Core) [OpenID.Core]). The jwks\_uri and jwks parameters MUST NOT be used together.

sector\_identifier\_uri

OPTIONAL. URL using the https scheme to be used in calculating Pseudonymous Identifiers by the OP. The URL references a file with a single JSON array of redirect\_uri values. Please see [Section 5 ("sector\_identifier\_uri" Validation)](#SectorIdentifierValidation). Providers that use pairwise sub (subject) values SHOULD utilize the sector\_identifier\_uri value provided in the Subject Identifier calculation for pairwise identifiers.

subject\_type

OPTIONAL. subject\_type requested for responses to this Client. The subject\_types\_supported Discovery parameter contains a list of the supported subject\_type values for this server. Valid types include pairwise and public.

id\_token\_signed\_response\_alg

OPTIONAL. JWS alg algorithm [[JWA] (Jones, M., “JSON Web Algorithms (JWA),” May 2015.)](" \l "JWA) REQUIRED for signing the ID Token issued to this Client. The value none MUST NOT be used as the ID Token alg value unless the Client uses only Response Types that return no ID Token from the Authorization Endpoint (such as when only using the Authorization Code Flow). The default, if omitted, is RS256. The public key for validating the signature is provided by retrieving the JWK Set referenced by the jwks\_uri element from [OpenID Connect Discovery 1.0 (Sakimura, N., Bradley, J., Jones, M., and E. Jay, “OpenID Connect Discovery 1.0,” August 2015.)](" \l "OpenID.Discovery) [OpenID.Discovery].

id\_token\_encrypted\_response\_alg

OPTIONAL. JWE alg algorithm [[JWA] (Jones, M., “JSON Web Algorithms (JWA),” May 2015.)](" \l "JWA) REQUIRED for encrypting the ID Token issued to this Client. If this is requested, the response will be signed then encrypted, with the result being a Nested JWT, as defined in [[JWT] (Jones, M., Bradley, J., and N. Sakimura, “JSON Web Token (JWT),” May 2015.)](" \l "JWT). The default, if omitted, is that no encryption is performed.

id\_token\_encrypted\_response\_enc

OPTIONAL. JWE enc algorithm [[JWA] (Jones, M., “JSON Web Algorithms (JWA),” May 2015.)](" \l "JWA) REQUIRED for encrypting the ID Token issued to this Client. If id\_token\_encrypted\_response\_alg is specified, the default id\_token\_encrypted\_response\_enc value is A128CBC-HS256. When id\_token\_encrypted\_response\_enc is included, id\_token\_encrypted\_response\_alg MUST also be provided.

userinfo\_signed\_response\_alg

OPTIONAL. JWS alg algorithm [[JWA] (Jones, M., “JSON Web Algorithms (JWA),” May 2015.)](" \l "JWA) REQUIRED for signing UserInfo Responses. If this is specified, the response will be [JWT (Jones, M., Bradley, J., and N. Sakimura, “JSON Web Token (JWT),” May 2015.)](" \l "JWT) [JWT] serialized, and signed using JWS. The default, if omitted, is for the UserInfo Response to return the Claims as a UTF-8 [[RFC3629] (Yergeau, F., “UTF-8, a transformation format of ISO 10646,” November 2003.)](" \l "RFC3629) encoded JSON object using the application/json content-type.

userinfo\_encrypted\_response\_alg

OPTIONAL. [JWE (Jones, M., Rescorla, E., and J. Hildebrand, “JSON Web Encryption (JWE),” May 2015.)](" \l "JWE) [JWE] alg algorithm [[JWA] (Jones, M., “JSON Web Algorithms (JWA),” May 2015.)](" \l "JWA) REQUIRED for encrypting UserInfo Responses. If both signing and encryption are requested, the response will be signed then encrypted, with the result being a Nested JWT, as defined in [[JWT] (Jones, M., Bradley, J., and N. Sakimura, “JSON Web Token (JWT),” May 2015.)](" \l "JWT). The default, if omitted, is that no encryption is performed.

userinfo\_encrypted\_response\_enc

OPTIONAL. JWE enc algorithm [[JWA] (Jones, M., “JSON Web Algorithms (JWA),” May 2015.)](" \l "JWA) REQUIRED for encrypting UserInfo Responses. If userinfo\_encrypted\_response\_alg is specified, the default userinfo\_encrypted\_response\_enc value is A128CBC-HS256. When userinfo\_encrypted\_response\_enc is included, userinfo\_encrypted\_response\_alg MUST also be provided.

request\_object\_signing\_alg

OPTIONAL. [JWS (Jones, M., Bradley, J., and N. Sakimura, “JSON Web Signature (JWS),” May 2015.)](" \l "JWS) [JWS] alg algorithm [[JWA] (Jones, M., “JSON Web Algorithms (JWA),” May 2015.)](" \l "JWA) that MUST be used for signing Request Objects sent to the OP. All Request Objects from this Client MUST be rejected, if not signed with this algorithm. Request Objects are described in Section 6.1 of [OpenID Connect Core 1.0 (Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and C. Mortimore, “OpenID Connect Core 1.0,” August 2015.)](" \l "OpenID.Core) [OpenID.Core]. This algorithm MUST be used both when the Request Object is passed by value (using the request parameter) and when it is passed by reference (using the request\_uri parameter). Servers SHOULD support RS256. The value none MAY be used. The default, if omitted, is that any algorithm supported by the OP and the RP MAY be used.

request\_object\_encryption\_alg

OPTIONAL. [JWE (Jones, M., Rescorla, E., and J. Hildebrand, “JSON Web Encryption (JWE),” May 2015.)](" \l "JWE) [JWE] alg algorithm [[JWA] (Jones, M., “JSON Web Algorithms (JWA),” May 2015.)](" \l "JWA) the RP is declaring that it may use for encrypting Request Objects sent to the OP. This parameter SHOULD be included when symmetric encryption will be used, since this signals to the OP that a client\_secret value needs to be returned from which the symmetric key will be derived, that might not otherwise be returned. The RP MAY still use other supported encryption algorithms or send unencrypted Request Objects, even when this parameter is present. If both signing and encryption are requested, the Request Object will be signed then encrypted, with the result being a Nested JWT, as defined in [[JWT] (Jones, M., Bradley, J., and N. Sakimura, “JSON Web Token (JWT),” May 2015.)](" \l "JWT). The default, if omitted, is that the RP is not declaring whether it might encrypt any Request Objects.

request\_object\_encryption\_enc

OPTIONAL. JWE enc algorithm [[JWA] (Jones, M., “JSON Web Algorithms (JWA),” May 2015.)](" \l "JWA) the RP is declaring that it may use for encrypting Request Objects sent to the OP. If request\_object\_encryption\_alg is specified, the default request\_object\_encryption\_enc value is A128CBC-HS256. When request\_object\_encryption\_enc is included, request\_object\_encryption\_alg MUST also be provided.

token\_endpoint\_auth\_method

OPTIONAL. Requested Client Authentication method for the Token Endpoint. The options are client\_secret\_post, client\_secret\_basic, client\_secret\_jwt, private\_key\_jwt, and none, as described in Section 9 of [OpenID Connect Core 1.0 (Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and C. Mortimore, “OpenID Connect Core 1.0,” August 2015.)](" \l "OpenID.Core) [OpenID.Core]. Other authentication methods MAY be defined by extensions. If omitted, the default is client\_secret\_basic -- the HTTP Basic Authentication Scheme specified in Section 2.3.1 of [OAuth 2.0 (Hardt, D., Ed., “The OAuth 2.0 Authorization Framework,” October 2012.)](" \l "RFC6749) [RFC6749].

token\_endpoint\_auth\_signing\_alg

OPTIONAL. [JWS (Jones, M., Bradley, J., and N. Sakimura, “JSON Web Signature (JWS),” May 2015.)](" \l "JWS) [JWS] alg algorithm [[JWA] (Jones, M., “JSON Web Algorithms (JWA),” May 2015.)](" \l "JWA) that MUST be used for signing the JWT [[JWT] (Jones, M., Bradley, J., and N. Sakimura, “JSON Web Token (JWT),” May 2015.)](" \l "JWT) used to authenticate the Client at the Token Endpoint for the private\_key\_jwt and client\_secret\_jwt authentication methods. All Token Requests using these authentication methods from this Client MUST be rejected, if the JWT is not signed with this algorithm. Servers SHOULD support RS256. The value none MUST NOT be used. The default, if omitted, is that any algorithm supported by the OP and the RP MAY be used.

default\_max\_age

OPTIONAL. Default Maximum Authentication Age. Specifies that the End-User MUST be actively authenticated if the End-User was authenticated longer ago than the specified number of seconds. The max\_age request parameter overrides this default value. If omitted, no default Maximum Authentication Age is specified.

require\_auth\_time

OPTIONAL. Boolean value specifying whether the auth\_time Claim in the ID Token is REQUIRED. It is REQUIRED when the value is true. (If this is false, the auth\_time Claim can still be dynamically requested as an individual Claim for the ID Token using the claims request parameter described in Section 5.5.1 of [OpenID Connect Core 1.0 (Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and C. Mortimore, “OpenID Connect Core 1.0,” August 2015.)](" \l "OpenID.Core) [OpenID.Core].) If omitted, the default value is false.

default\_acr\_values

OPTIONAL. Default requested Authentication Context Class Reference values. Array of strings that specifies the default acr values that the OP is being requested to use for processing requests from this Client, with the values appearing in order of preference. The Authentication Context Class satisfied by the authentication performed is returned as the acr Claim Value in the issued ID Token. The acr Claim is requested as a Voluntary Claim by this parameter. The acr\_values\_supported discovery element contains a list of the supported acr values supported by this server. Values specified in the acr\_values request parameter or an individual acr Claim request override these default values.

initiate\_login\_uri

OPTIONAL. URI using the https scheme that a third party can use to initiate a login by the RP, as specified in Section 4 of [OpenID Connect Core 1.0 (Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and C. Mortimore, “OpenID Connect Core 1.0,” August 2015.)](" \l "OpenID.Core) [OpenID.Core]. The URI MUST accept requests via both GET and POST. The Client MUST understand the login\_hint and iss parameters and SHOULD support the target\_link\_uri parameter.

request\_uris

OPTIONAL. Array of request\_uri values that are pre-registered by the RP for use at the OP. Servers MAY cache the contents of the files referenced by these URIs and not retrieve them at the time they are used in a request. OPs can require that request\_uri values used be pre-registered with the require\_request\_uri\_registration discovery parameter.

If the contents of the request file could ever change, these URI values SHOULD include the base64url-encoded SHA-256 hash value of the file contents referenced by the URI as the value of the URI fragment. If the fragment value used for a URI changes, that signals the server that its cached value for that URI with the old fragment value is no longer valid.

Additional Client Metadata parameters MAY also be used. Some are defined by other specifications, such as [OpenID Connect Session Management 1.0 (Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and N. Agarwal, “OpenID Connect Session Management 1.0,” August 2015.)](" \l "OpenID.Session) [OpenID.Session].

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

### 2.1.  Metadata Languages and Scripts

Human-readable Client Metadata values and Client Metadata values that reference human-readable values MAY be represented in multiple languages and scripts. For example, values such as client\_name, tos\_uri, policy\_uri, logo\_uri, and client\_uri might have multiple locale-specific values in some Client registrations.

To specify the languages and scripts, [BCP47 (Phillips, A., Ed. and M. Davis, Ed., “Tags for Identifying Languages,” September 2009.)](" \l "RFC5646) [RFC5646] language tags are added to Client Metadata member names, delimited by a # character. The same syntax is used for representing languages and scripts for Client Metadata as is used for Claims, as described in Section 5.2 (Claims Languages and Scripts) of [OpenID Connect Core 1.0 (Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and C. Mortimore, “OpenID Connect Core 1.0,” August 2015.)](" \l "OpenID.Core) [OpenID.Core].

If such a human-readable field is sent without a language tag, parties using it MUST NOT make any assumptions about the language, character set, or script of the string value, and the string value MUST be used as-is wherever it is presented in a user interface. To facilitate interoperability, it is RECOMMENDED that any human-readable fields sent without language tags contain values suitable for display on a wide variety of systems.

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

### 3.  Client Registration Endpoint

The Client Registration Endpoint is an OAuth 2.0 Protected Resource through which a new Client registration can be requested. The OpenID Provider MAY require an Initial Access Token that is provisioned out-of-band (in a manner that is out of scope for this specification) to restrict registration requests to only authorized Clients or developers.

To support open Dynamic Registration, the Client Registration Endpoint SHOULD accept registration requests without OAuth 2.0 Access Tokens. These requests MAY be rate-limited or otherwise limited to prevent a denial-of-service attack on the Client Registration Endpoint. If an Initial Access Token is required for Client registration, the Client Registration Endpoint MUST be able to accept these Access Tokens in the manner described in the [OAuth 2.0 Bearer Token Usage (Jones, M. and D. Hardt, “The OAuth 2.0 Authorization Framework: Bearer Token Usage,” October 2012.)](#RFC6750) [RFC6750] specification.

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

### 3.1.  Client Registration Request

To register a new Client at the Authorization Server, the Client sends an HTTP POST message to the Client Registration Endpoint with any Client Metadata parameters that the Client chooses to specify for itself during the registration. The Authorization Server assigns this Client a unique Client Identifier, optionally assigns a Client Secret, and associates the Metadata given in the request with the issued Client Identifier. The Authorization Server MAY provision default values for any items omitted in the Client Metadata.

The Client sends an HTTP POST to the Client Registration Endpoint with a content type of application/json with the parameters represented as top-level members of the root JSON object.

The following is a non-normative example registration request (with line wraps within values for display purposes only):

POST /connect/register HTTP/1.1

Content-Type: application/json

Accept: application/json

Host: server.example.com

Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJ ...

{

"application\_type": "web",

"redirect\_uris":

["https://client.example.org/callback",

"https://client.example.org/callback2"],

"client\_name": "My Example",

"client\_name#ja-Jpan-JP":

"クライアント名",

"logo\_uri": "https://client.example.org/logo.png",

"subject\_type": "pairwise",

"sector\_identifier\_uri":

"https://other.example.net/file\_of\_redirect\_uris.json",

"token\_endpoint\_auth\_method": "client\_secret\_basic",

"jwks\_uri": "https://client.example.org/my\_public\_keys.jwks",

"userinfo\_encrypted\_response\_alg": "RSA1\_5",

"userinfo\_encrypted\_response\_enc": "A128CBC-HS256",

"contacts": ["ve7jtb@example.org", "mary@example.org"],

"request\_uris":

["https://client.example.org/rf.txt

#qpXaRLh\_n93TTR9F252ValdatUQvQiJi5BDub2BeznA"]

}

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

### 3.2.  Client Registration Response

Upon successful registration, the Client Registration Endpoint returns the newly-created Client Identifier and, if applicable, a Client Secret, along with all registered Metadata about this Client, including any fields provisioned by the Authorization Server itself. The Authorization Server MAY reject or replace any of the Client's requested field values and substitute them with suitable values. If this happens, the Authorization Server MUST include these fields in the response to the Client. An Authorization Server MAY ignore values provided by the client, and MUST ignore any fields sent by the Client that it does not understand.

The response MAY contain a Registration Access Token that can be used by the Client to perform subsequent operations upon the resulting Client registration.

A successful response SHOULD use the HTTP 201 Created status code and return a JSON document [[RFC4627] (Crockford, D., “The application/json Media Type for JavaScript Object Notation (JSON),” July 2006.)](#RFC4627) using the application/json content type with the following fields and the Client Metadata parameters as top-level members of the root JSON object:

client\_id

REQUIRED. Unique Client Identifier. It MUST NOT be currently valid for any other registered Client.

client\_secret

OPTIONAL. Client Secret. The same Client Secret value MUST NOT be assigned to multiple Clients. This value is used by Confidential Clients to authenticate to the Token Endpoint, as described in Section 2.3.1 of OAuth 2.0, and for the derivation of symmetric encryption key values, as described in Section 10.2 of [OpenID Connect Core 1.0 (Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and C. Mortimore, “OpenID Connect Core 1.0,” August 2015.)](" \l "OpenID.Core) [OpenID.Core]. It is not needed for Clients selecting a token\_endpoint\_auth\_method of private\_key\_jwt unless symmetric encryption will be used.

registration\_access\_token

OPTIONAL. Registration Access Token that can be used at the Client Configuration Endpoint to perform subsequent operations upon the Client registration.

registration\_client\_uri

OPTIONAL. Location of the Client Configuration Endpoint where the Registration Access Token can be used to perform subsequent operations upon the resulting Client registration. Implementations MUST either return both a Client Configuration Endpoint and a Registration Access Token or neither of them.

client\_id\_issued\_at

OPTIONAL. Time at which the Client Identifier was issued. Its value is a JSON number representing the number of seconds from 1970-01-01T00:00:00Z as measured in UTC until the date/time.

client\_secret\_expires\_at

REQUIRED if client\_secret is issued. Time at which the client\_secret will expire or 0 if it will not expire. Its value is a JSON number representing the number of seconds from 1970-01-01T00:00:00Z as measured in UTC until the date/time.

The following is a non-normative example registration response (with line wraps within values for display purposes only):

HTTP/1.1 201 Created

Content-Type: application/json

Cache-Control: no-cache, no-store

Pragma: no-cache

{

"client\_id": "s6BhdRkqt3",

"client\_secret":

"ZJYCqe3GGRvdrudKyZS0XhGv\_Z45DuKhCUk0gBR1vZk",

"client\_secret\_expires\_at": 1577858400,

"registration\_access\_token":

"this.is.an.access.token.value.ffx83",

"registration\_client\_uri":

"https://server.example.com/connect/register?client\_id=s6BhdRkqt3",

"token\_endpoint\_auth\_method":

"client\_secret\_basic",

"application\_type": "web",

"redirect\_uris":

["https://client.example.org/callback",

"https://client.example.org/callback2"],

"client\_name": "My Example",

"client\_name#ja-Jpan-JP":

"クライアント名",

"logo\_uri": "https://client.example.org/logo.png",

"subject\_type": "pairwise",

"sector\_identifier\_uri":

"https://other.example.net/file\_of\_redirect\_uris.json",

"jwks\_uri": "https://client.example.org/my\_public\_keys.jwks",

"userinfo\_encrypted\_response\_alg": "RSA1\_5",

"userinfo\_encrypted\_response\_enc": "A128CBC-HS256",

"contacts": ["ve7jtb@example.org", "mary@example.org"],

"request\_uris":

["https://client.example.org/rf.txt

#qpXaRLh\_n93TTR9F252ValdatUQvQiJi5BDub2BeznA"]

}

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

### 3.3.  Client Registration Error Response

When an OAuth error condition occurs, the Client Registration Endpoint returns an Error Response as defined in Section 3 of the [OAuth 2.0 Bearer Token Usage (Jones, M. and D. Hardt, “The OAuth 2.0 Authorization Framework: Bearer Token Usage,” October 2012.)](#RFC6750) [RFC6750] specification.

When a registration error condition occurs, the Client Registration Endpoint returns a HTTP 400 Bad Request status code including a JSON object describing the error in the response body.

The JSON object describing the error contains two members:

error

Error code.

error\_description

Additional text description of the error for debugging.

Other members MAY also be used.

This specification defines the following error codes:

invalid\_redirect\_uri

The value of one or more redirect\_uris is invalid.

invalid\_client\_metadata

The value of one of the Client Metadata fields is invalid and the server has rejected this request. Note that an Authorization Server MAY choose to substitute a valid value for any requested parameter of a Client's Metadata.

Other error codes MAY also be used.

The following is a non-normative example error response:

HTTP/1.1 400 Bad Request

Content-Type: application/json

Cache-Control: no-cache, no-store

Pragma: no-cache

{

"error": "invalid\_redirect\_uri",

"error\_description": "One or more redirect\_uri values are invalid"

}

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

### 4.  Client Configuration Endpoint

The Client Configuration Endpoint is an OAuth 2.0 Protected Resource that MAY be provisioned by the server for a specific Client to be able to view and update its registered information. The Client MUST use its Registration Access Token in all calls to this endpoint as an OAuth 2.0 Bearer Token [[RFC6750] (Jones, M. and D. Hardt, “The OAuth 2.0 Authorization Framework: Bearer Token Usage,” October 2012.)](#RFC6750).

Operations on this endpoint are switched through the use of different HTTP methods [[RFC7231] (Fielding, R., Ed. and J. Reschke, Ed., “Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content,” June 2014.)](" \l "RFC7231). The only method defined for use at this endpoint by this specification is the HTTP GET method.

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

### 4.1.  Forming the Client Configuration Endpoint URL

If a Client Configuration Endpoint and a Registration Access Token are returned by the initial registration of the Client, the Authorization Server MUST provide the Client with the fully qualified URL in the registration\_client\_uri element of the Client Registration Response, per [Section 3.2 (Client Registration Response)](#RegistrationResponse). The Authorization Server MUST NOT expect the Client to construct or discover this URL on its own. The Client MUST use the URL as given by the server and MUST NOT construct this URL from component pieces.

Depending on deployment characteristics, the Client Configuration Endpoint URL can take any number of forms. It is RECOMMENDED that this endpoint URL be formed through the use of a server-constructed URL string which combines the Client Registration Endpoint's URL and the issued Client ID for this Client, with the latter as either a path parameter or a query parameter. For example, a Client with the Client ID s6BhdRkqt3 could be given a Client Configuration Endpoint URL of https://server.example.com/register/s6BhdRkqt3 (path parameter) or of https://server.example.com/register?client\_id=s6BhdRkqt3 (query parameter). In both of these cases, the Client simply uses the URL as given.

These common patterns can help the Server to more easily determine the Client to which the request pertains, which MUST be matched against the Client to which the Registration Access Token was issued. If desired, the Server MAY simply return the Client Registration Endpoint URL as the Client Configuration Endpoint URL and change behavior based on the authentication context provided by the Registration Access Token.

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

### 4.2.  Client Read Request

If the initial registration of the Client returned a Client Configuration Endpoint and a Registration Access Token, the current configuration of the Client on the Authorization Server can be read by making an HTTP GET request to the Client Configuration Endpoint with the Registration Access Token. This operation SHOULD be idempotent -- not causing changes to the Client configuration.

The following is a non-normative example read request:

GET /connect/register?client\_id=s6BhdRkqt3 HTTP/1.1

Accept: application/json

Host: server.example.com

Authorization: Bearer this.is.an.access.token.value.ffx83

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

### 4.3.  Client Read Response

Upon a successful read operation, the Authorization Server SHOULD return all registered Metadata about this Client, including any fields provisioned by the Authorization Server itself. Note that some values, including the client\_secret value, might have been updated since the initial registration. The mechanisms for such updates are beyond the scope of this specification. However, since Read operations are intended to be idempotent, the Client Read Request itself SHOULD NOT cause changes to the Client's registered Metadata values.

The Authorization Server need not include the registration\_access\_token or registration\_client\_uri value in this response unless they have been updated.

A successful response SHOULD use the HTTP 200 OK status code and return a JSON document [[RFC4627] (Crockford, D., “The application/json Media Type for JavaScript Object Notation (JSON),” July 2006.)](#RFC4627) using the application/json content type with the Client Metadata values as top-level members of the root JSON object.

The following is a non-normative example read response (with line wraps within values for display purposes only):

HTTP/1.1 200 OK

Content-Type: application/json

Cache-Control: no-cache, no-store

Pragma: no-cache

{

"client\_id": "s6BhdRkqt3",

"client\_secret":

"OylyaC56ijpAQ7G5ZZGL7MMQ6Ap6mEeuhSTFVps2N4Q",

"client\_secret\_expires\_at": 17514165600,

"registration\_client\_uri":

"https://server.example.com/connect/register?client\_id=s6BhdRkqt3",

"token\_endpoint\_auth\_method":

"client\_secret\_basic",

"application\_type": "web",

"redirect\_uris":

["https://client.example.org/callback",

"https://client.example.org/callback2"],

"client\_name": "My Example",

"client\_name#ja-Jpan-JP":

"クライアント名",

"logo\_uri": "https://client.example.org/logo.png",

"subject\_type": "pairwise",

"sector\_identifier\_uri":

"https://other.example.net/file\_of\_redirect\_uris.json",

"jwks\_uri": "https://client.example.org/my\_public\_keys.jwks",

"userinfo\_encrypted\_response\_alg": "RSA1\_5",

"userinfo\_encrypted\_response\_enc": "A128CBC-HS256",

"contacts": ["ve7jtb@example.org", "mary@example.org"],

"request\_uris":

["https://client.example.org/rf.txt

#qpXaRLh\_n93TTR9F252ValdatUQvQiJi5BDub2BeznA"]

}

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

### 4.4.  Client Read Error Response

If the Registration Access Token used to make this request is not valid, the server MUST respond with an error as described in [OAuth Bearer Token Usage (Jones, M. and D. Hardt, “The OAuth 2.0 Authorization Framework: Bearer Token Usage,” October 2012.)](#RFC6750) [RFC6750].

If the Client does not exist on this server, the Client is invalid, or the Registration Access Token used is invalid, the server MUST respond with the HTTP 401 Unauthorized status code. If the Client does not have permission to read its record, the server MUST return an HTTP 403 Forbidden. Note that for security reasons, to inhibit brute force attacks, endpoints MUST NOT return the HTTP 404 Not Found status code.

The following is a non-normative example error response:

HTTP/1.1 401 Unauthorized

WWW-Authenticate: Bearer error="invalid\_token",

error\_description="The access token expired"

Cache-Control: no-cache, no-store

Pragma: no-cache

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

### 5.  "sector\_identifier\_uri" Validation

The sector identifier list provides a way for a group of Web sites under single administrative control to have consistent pairwise sub values, independent of their domain names, as described in Section 8.1 of [OpenID Connect Core 1.0 (Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and C. Mortimore, “OpenID Connect Core 1.0,” August 2015.)](" \l "OpenID.Core) [OpenID.Core]. It also provides a way for Clients to change redirect\_uri domains without having to re-register all of their users.

The value of the sector\_identifier\_uri MUST be a URL using the https scheme that references a JSON file containing an array of redirect\_uri values. The values registered in redirect\_uris MUST be included in the elements of the array, or registration MUST fail. This MUST be validated at registration time; there is no requirement for the OP to retain the contents of this JSON file or to retrieve or revalidate its contents in the future.

The following is a non-normative example request to and reply from a sector\_identifier\_uri:

GET /file\_of\_redirect\_uris.json HTTP/1.1

Accept: application/json

Host: other.example.net

HTTP/1.1 200 OK

Content-Type: application/json

Cache-Control: no-cache, no-store

Pragma: no-cache

[ "https://client.example.org/callback",

"https://client.example.org/callback2",

"https://client.other\_company.example.net/callback" ]

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

### 6.  String Operations

Processing some OpenID Connect messages requires comparing values in the messages to known values. For example, the member names in the Client registration response might be compared to specific member names such as client\_id. Comparing Unicode [[UNICODE] (The Unicode Consortium, “The Unicode Standard,” .)](" \l "UNICODE) strings, however, has significant security implications.

Therefore, comparisons between JSON strings and other Unicode strings MUST be performed as specified below:

1. Remove any JSON applied escaping to produce an array of Unicode code points.
2. Unicode Normalization [[USA15] (Davis, M. and K. Whistler, “Unicode Normalization Forms,” 06 2015.)](" \l "USA15) MUST NOT be applied at any point to either the JSON string or to the string it is to be compared against.
3. Comparisons between the two strings MUST be performed as a Unicode code point to code point equality comparison.

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

### 7.  Validation

If any of the validation procedures defined in this specification fail, any operations requiring the information that failed to correctly validate MUST be aborted and the information that failed to validate MUST NOT be used.

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

### 8.  Implementation Considerations

This specification defines features used by both Relying Parties and OpenID Providers that choose to implement Dynamic Client Registration. All of these Relying Parties and OpenID Providers MUST implement the features that are listed in this specification as being "REQUIRED" or are described with a "MUST".

This specification is compatible with the [OAuth 2.0 Dynamic Client Registration Protocol (Richer, J., Ed., Jones, M., Bradley, J., Machulak, M., and P. Hunt, “OAuth 2.0 Dynamic Client Registration Protocol,” July 2015.)](" \l "RFC7591) [RFC7591]. Implementations MAY use additional Client Metadata values defined by [[RFC7591] (Richer, J., Ed., Jones, M., Bradley, J., Machulak, M., and P. Hunt, “OAuth 2.0 Dynamic Client Registration Protocol,” July 2015.)](" \l "RFC7591), such as software\_statement, should they facilitate their use cases. Implementations wanting to support additional operations defined in [OAuth 2.0 Dynamic Client Registration Management Protocol (Richer, J., Ed., Jones, M., Bradley, J., and M. Machulak, “OAuth 2.0 Dynamic Client Registration Management Protocol,” July 2015.)](" \l "RFC7592) [RFC7592], such as Update, can do so using that specification, while being mindful that the specification is experimental.

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

### 8.1.  Compatibility Notes

NOTE: Potential compatibility issues that were previously described in the original version of this specification have since been addressed.

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

### 8.2.  Implementation Notes on Stateless Dynamic Client Registration

In some deployments, it is advantageous to enable Clients to obtain the information necessary to interact with the Authorization Server, such as a Client Identifier, without the requirement that state about the Client be stored at the Authorization Server. The interfaces defined by this specification can be used for stateless dynamic client registration.

One means of doing this is to encode necessary registration information about the Client into the client\_id value returned by the initial registration of the Client. This has the effect of having the Client store this information, rather than the Authorization Server. The particular encodings used by different Authorization Servers will differ.

When stateless dynamic client registration is used by the Authorization Server, read operations are likely to not be possible, because issuing a Registration Access Token might require per-Client state at the Authorization Server. In that case, no Client Configuration Endpoint or Registration Access Token will be returned by the initial registration of the Client.

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

### 9.  Security Considerations

Since requests to the Client Registration Endpoint result in the transmission of clear-text credentials (in the HTTP request and response), all communication with the Registration Endpoint MUST utilize TLS. See [Section 9.3 (TLS Requirements)](#TLSRequirements) for more information on using TLS.

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

### 9.1.  Impersonation

A rogue RP might use the logo for the legitimate RP, which it is trying to impersonate. An OP needs to take steps to mitigate this phishing risk, since the logo could confuse users into thinking they're logging in to the legitimate RP. An OP could also warn if the domain/site of the logo doesn't match the domain/site of registered Redirection URIs. An OP can also make warnings against untrusted RPs in all cases, especially if they're dynamically registered, have not been trusted by any users at the OP before, and want to use the logo feature.

In a situation where the Authorization Server is supporting open Client registration, it needs to be extremely careful with any URL provided by the Client that will be displayed to the End-User (e.g. logo\_uri and policy\_uri). A rogue Client could specify a registration request with a reference to a drive-by download in the policy\_uri. The Authorization Server SHOULD check to see if the logo\_uri and policy\_uri have the same host as the hosts defined in the array of redirect\_uris.

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

### 9.2.  Native Code Leakage

Implementers should be aware that on iOS, information is returned to native applications using custom URI schemes, but multiple applications can register the same URI scheme. In this case, it is nondeterministic which application receives the information. This can result in an Authorization Code being leaked to the wrong application. Several possible solutions to this have been proposed and are being discussed in the IETF OAuth working group. It is expected that a standard solution to this problem will be developed there. At that point, an extension to OpenID Connect may be published describing how to apply that solution to OpenID Connect.

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

### 9.3.  TLS Requirements

Implementations MUST support TLS. Which version(s) ought to be implemented will vary over time, and depend on the widespread deployment and known security vulnerabilities at the time of implementation. At the time of this writing, TLS version 1.2 [[RFC5246] (Dierks, T. and E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.2,” August 2008.)](#RFC5246) is the most recent version, but has very limited actual deployment, and might not be readily available in implementation toolkits. TLS version 1.0 [[RFC2246] (Dierks, T. and C. Allen, “The TLS Protocol Version 1.0,” January 1999.)](#RFC2246) is the most widely deployed version, and will give the broadest interoperability.

To protect against information disclosure and tampering, confidentiality protection MUST be applied using TLS with a ciphersuite that provides confidentiality and integrity protection.

Whenever TLS is used, a TLS server certificate check MUST be performed, per [RFC 6125 (Saint-Andre, P. and J. Hodges, “Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS),” March 2011.)](#RFC6125) [RFC6125].

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

### 10.  IANA Considerations

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

### 10.1.  OAuth Dynamic Client Registration Metadata Registration

This specification registers the following client metadata definitions in the IANA "OAuth Dynamic Client Registration Metadata" registry [[IANA.OAuth.Parameters] (IANA, “OAuth Parameters,” .)](" \l "IANA.OAuth.Parameters) established by [[RFC7591] (Richer, J., Ed., Jones, M., Bradley, J., Machulak, M., and P. Hunt, “OAuth 2.0 Dynamic Client Registration Protocol,” July 2015.)](" \l "RFC7591):

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

### 10.1.1.  Registry Contents

* Client Metadata Name: application\_type
* Client Metadata Description: Kind of the application -- "native" or "web"
* Change Controller: OpenID Foundation Artifact Binding Working Group - openid-specs-ab@lists.openid.net
* Specification Document(s): [Section 2 (Client Metadata)](" \l "ClientMetadata) of this document
* Client Metadata Name: sector\_identifier\_uri
* Client Metadata Description: URL using the https scheme to be used in calculating Pseudonymous Identifiers by the OP
* Change Controller: OpenID Foundation Artifact Binding Working Group - openid-specs-ab@lists.openid.net
* Specification Document(s): [Section 2 (Client Metadata)](" \l "ClientMetadata) of this document
* Client Metadata Name: subject\_type
* Client Metadata Description: subject\_type requested for responses to this Client -- "pairwise" or "public"
* Change Controller: OpenID Foundation Artifact Binding Working Group - openid-specs-ab@lists.openid.net
* Specification Document(s): [Section 2 (Client Metadata)](" \l "ClientMetadata) of this document
* Client Metadata Name: id\_token\_signed\_response\_alg
* Client Metadata Description: JWS alg algorithm REQUIRED for signing the ID Token issued to this Client
* Change Controller: OpenID Foundation Artifact Binding Working Group - openid-specs-ab@lists.openid.net
* Specification Document(s): [Section 2 (Client Metadata)](" \l "ClientMetadata) of this document
* Client Metadata Name: id\_token\_encrypted\_response\_alg
* Client Metadata Description: JWE alg algorithm REQUIRED for encrypting the ID Token issued to this Client
* Change Controller: OpenID Foundation Artifact Binding Working Group - openid-specs-ab@lists.openid.net
* Specification Document(s): [Section 2 (Client Metadata)](" \l "ClientMetadata) of this document
* Client Metadata Name: id\_token\_encrypted\_response\_enc
* Client Metadata Description: JWE enc algorithm REQUIRED for encrypting the ID Token issued to this Client
* Change Controller: OpenID Foundation Artifact Binding Working Group - openid-specs-ab@lists.openid.net
* Specification Document(s): [Section 2 (Client Metadata)](" \l "ClientMetadata) of this document
* Client Metadata Name: userinfo\_signed\_response\_alg
* Client Metadata Description: JWS alg algorithm REQUIRED for signing UserInfo Responses
* Change Controller: OpenID Foundation Artifact Binding Working Group - openid-specs-ab@lists.openid.net
* Specification Document(s): [Section 2 (Client Metadata)](" \l "ClientMetadata) of this document
* Client Metadata Name: userinfo\_encrypted\_response\_alg
* Client Metadata Description: JWE alg algorithm REQUIRED for encrypting UserInfo Responses
* Change Controller: OpenID Foundation Artifact Binding Working Group - openid-specs-ab@lists.openid.net
* Specification Document(s): [Section 2 (Client Metadata)](" \l "ClientMetadata) of this document
* Client Metadata Name: userinfo\_encrypted\_response\_enc
* Client Metadata Description: JWE enc algorithm REQUIRED for encrypting UserInfo Responses
* Change Controller: OpenID Foundation Artifact Binding Working Group - openid-specs-ab@lists.openid.net
* Specification Document(s): [Section 2 (Client Metadata)](" \l "ClientMetadata) of this document
* Client Metadata Name: request\_object\_signing\_alg
* Client Metadata Description: JWS alg algorithm that MUST be used for signing Request Objects sent to the OP
* Change Controller: OpenID Foundation Artifact Binding Working Group - openid-specs-ab@lists.openid.net
* Specification Document(s): [Section 2 (Client Metadata)](" \l "ClientMetadata) of this document
* Client Metadata Name: request\_object\_encryption\_alg
* Client Metadata Description: JWE alg algorithm the RP is declaring that it may use for encrypting Request Objects sent to the OP
* Change Controller: OpenID Foundation Artifact Binding Working Group - openid-specs-ab@lists.openid.net
* Specification Document(s): [Section 2 (Client Metadata)](" \l "ClientMetadata) of this document
* Client Metadata Name: request\_object\_encryption\_enc
* Client Metadata Description: JWE enc algorithm the RP is declaring that it may use for encrypting Request Objects sent to the OP
* Change Controller: OpenID Foundation Artifact Binding Working Group - openid-specs-ab@lists.openid.net
* Specification Document(s): [Section 2 (Client Metadata)](" \l "ClientMetadata) of this document
* Client Metadata Name: token\_endpoint\_auth\_signing\_alg
* Client Metadata Description: JWS alg algorithm that MUST be used for signing the JWT used to authenticate the Client at the Token Endpoint for the private\_key\_jwt and client\_secret\_jwt authentication methods
* Change Controller: OpenID Foundation Artifact Binding Working Group - openid-specs-ab@lists.openid.net
* Specification Document(s): [Section 2 (Client Metadata)](" \l "ClientMetadata) of this document
* Client Metadata Name: default\_max\_age
* Client Metadata Description: Default Maximum Authentication Age
* Change Controller: OpenID Foundation Artifact Binding Working Group - openid-specs-ab@lists.openid.net
* Specification Document(s): [Section 2 (Client Metadata)](" \l "ClientMetadata) of this document
* Client Metadata Name: require\_auth\_time
* Client Metadata Description: Boolean value specifying whether the auth\_time Claim in the ID Token is REQUIRED
* Change Controller: OpenID Foundation Artifact Binding Working Group - openid-specs-ab@lists.openid.net
* Specification Document(s): [Section 2 (Client Metadata)](" \l "ClientMetadata) of this document
* Client Metadata Name: default\_acr\_values
* Client Metadata Description: Default requested Authentication Context Class Reference values
* Change Controller: OpenID Foundation Artifact Binding Working Group - openid-specs-ab@lists.openid.net
* Specification Document(s): [Section 2 (Client Metadata)](" \l "ClientMetadata) of this document
* Client Metadata Name: initiate\_login\_uri
* Client Metadata Description: URI using the https scheme that a third party can use to initiate a login by the RP
* Change Controller: OpenID Foundation Artifact Binding Working Group - openid-specs-ab@lists.openid.net
* Specification Document(s): [Section 2 (Client Metadata)](" \l "ClientMetadata) of this document
* Client Metadata Name: request\_uris
* Client Metadata Description: Array of request\_uri values that are pre-registered by the RP for use at the OP
* Change Controller: OpenID Foundation Artifact Binding Working Group - openid-specs-ab@lists.openid.net
* Specification Document(s): [Section 2 (Client Metadata)](" \l "ClientMetadata) of this document

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

### 10.2.  OAuth Token Endpoint Authentication Methods Registration

This specification registers the following token endpoint authentication methods in the IANA "OAuth Token Endpoint Authentication Methods" registry [[IANA.OAuth.Parameters] (IANA, “OAuth Parameters,” .)](" \l "IANA.OAuth.Parameters) established by [[RFC7591] (Richer, J., Ed., Jones, M., Bradley, J., Machulak, M., and P. Hunt, “OAuth 2.0 Dynamic Client Registration Protocol,” July 2015.)](" \l "RFC7591):

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

### 10.2.1.  Registry Contents

* Token Endpoint Authentication Method Name: client\_secret\_jwt
* Change Controller: OpenID Foundation Artifact Binding Working Group - openid-specs-ab@lists.openid.net
* Specification Document(s): Section 9 of OpenID Connect Core 1.0 [[OpenID.Core] (Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and C. Mortimore, “OpenID Connect Core 1.0,” August 2015.)](" \l "OpenID.Core)
* Token Endpoint Authentication Method Name: private\_key\_jwt
* Change Controller: OpenID Foundation Artifact Binding Working Group - openid-specs-ab@lists.openid.net
* Specification Document(s): Section 9 of OpenID Connect Core 1.0 [[OpenID.Core] (Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and C. Mortimore, “OpenID Connect Core 1.0,” August 2015.)](" \l "OpenID.Core)

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

### 11.  References

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

### 11.1. Normative References

|  |  |
| --- | --- |
| **[IANA.OAuth.Parameters]** | IANA, “[OAuth Parameters](http://www.iana.org/assignments/oauth-parameters).” |
| **[JWA]** | Jones, M., “[JSON Web Algorithms (JWA)](http://tools.ietf.org/html/rfc7518),” RFC 7518, DOI 10.17487/RFC7518, May 2015. |
| **[JWE]** | Jones, M., Rescorla, E., and J. Hildebrand, “[JSON Web Encryption (JWE)](http://tools.ietf.org/html/rfc7516),” RFC 7516, DOI 10.17487/RFC7516, May 2015. |
| **[JWK]** | “[JSON Web Key (JWK)](http://tools.ietf.org/html/rfc7517),” RFC 7517, DOI 10.17487/RFC7517, May 2015. |
| **[JWS]** | Jones, M., Bradley, J., and N. Sakimura, “[JSON Web Signature (JWS)](http://tools.ietf.org/html/rfc7515),” RFC 7515, DOI 10.17487/RFC7515, May 2015. |
| **[JWT]** | Jones, M., Bradley, J., and N. Sakimura, “[JSON Web Token (JWT)](http://tools.ietf.org/html/rfc7519),” RFC 7519, DOI 10.17487/RFC7519, May 2015. |
| **[OpenID.Core]** | Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and C. Mortimore, “[OpenID Connect Core 1.0](http://openid.net/specs/openid-connect-core-1_0.html),” August 2015. |
| **[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),” August 2015. |
| **[RFC2119]** | Bradner, S., “[Key words for use in RFCs to Indicate Requirement Levels](http://www.rfc-editor.org/info/rfc2119),” BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997. |
| **[RFC2246]** | Dierks, T. and C. Allen, “[The TLS Protocol Version 1.0](http://www.rfc-editor.org/info/rfc2246),” RFC 2246, DOI 10.17487/RFC2246, January 1999. |
| **[RFC3629]** | Yergeau, F., “[UTF-8, a transformation format of ISO 10646](http://www.rfc-editor.org/info/rfc3629),” STD 63, RFC 3629, DOI 10.17487/RFC3629, November 2003. |
| **[RFC3986]** | Berners-Lee, T., Fielding, R., and L. Masinter, “[Uniform Resource Identifier (URI): Generic Syntax](http://www.rfc-editor.org/info/rfc3986),” STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005. |
| **[RFC4627]** | Crockford, D., “[The application/json Media Type for JavaScript Object Notation (JSON)](http://www.rfc-editor.org/info/rfc4627),” RFC 4627, DOI 10.17487/RFC4627, July 2006. |
| **[RFC5246]** | Dierks, T. and E. Rescorla, “[The Transport Layer Security (TLS) Protocol Version 1.2](http://www.rfc-editor.org/info/rfc5246),” RFC 5246, DOI 10.17487/RFC5246, August 2008. |
| **[RFC5646]** | Phillips, A., Ed. and M. Davis, Ed., “[Tags for Identifying Languages](http://www.rfc-editor.org/info/rfc5646),” BCP 47, RFC 5646, DOI 10.17487/RFC5646, September 2009. |
| **[RFC6125]** | Saint-Andre, P. and J. Hodges, “[Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)](http://www.rfc-editor.org/info/rfc6125),” RFC 6125, DOI 10.17487/RFC6125, March 2011. |
| **[RFC6749]** | Hardt, D., Ed., “[The OAuth 2.0 Authorization Framework](http://www.rfc-editor.org/info/rfc6749),” RFC 6749, DOI 10.17487/RFC6749, October 2012. |
| **[RFC6750]** | Jones, M. and D. Hardt, “[The OAuth 2.0 Authorization Framework: Bearer Token Usage](http://www.rfc-editor.org/info/rfc6750),” RFC 6750, DOI 10.17487/RFC6750, October 2012. |
| **[RFC7159]** | Bray, T., Ed., “[The JavaScript Object Notation (JSON) Data Interchange Format](http://www.rfc-editor.org/info/rfc7159),” RFC 7159, DOI 10.17487/RFC7159, March 2014. |
| **[RFC7231]** | Fielding, R., Ed. and J. Reschke, Ed., “[Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content](http://www.rfc-editor.org/info/rfc7231),” RFC 7231, DOI 10.17487/RFC7231, June 2014. |
| **[UNICODE]** | The Unicode Consortium, “[The Unicode Standard](http://www.unicode.org/versions/latest/).” |
| **[USA15]** | [Davis, M.](mailto:markdavis@google.com) and [K. Whistler](mailto:ken@unicode.org), “[Unicode Normalization Forms](http://www.unicode.org/reports/tr15/),” Unicode Standard Annex 15, 06 2015. |

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

### 11.2. Informative References

|  |  |
| --- | --- |
| **[OpenID.Session]** | August 2015. |
| **[RFC7591]** | Richer, J., Ed., Jones, M., Bradley, J., Machulak, M., and P. Hunt, “[OAuth 2.0 Dynamic Client Registration Protocol](http://www.rfc-editor.org/info/rfc7591),” RFC 7591, DOI 10.17487/RFC7591, July 2015. |
| **[RFC7592]** | Richer, J., Ed., Jones, M., Bradley, J., and M. Machulak, “[OAuth 2.0 Dynamic Client Registration Management Protocol](http://www.rfc-editor.org/info/rfc7592),” RFC 7592, DOI 10.17487/RFC7592, July 2015. |

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

### Appendix A.  Acknowledgements

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

Amanda Anganes (aanganes@mitre.org), MITRE

John Bradley (ve7jtb@ve7jtb.com), Ping Identity

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

Vladimir Dzhuvinov (vladimir@nimbusds.com), Nimbus Directory Services

George Fletcher (george.fletcher@corp.aol.com), AOL

Roland Hedberg (roland.hedberg@adm.umu.se), University of Umea

Edmund Jay (ejay@mgi1.com), Illumila

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

Torsten Lodderstedt (t.lodderstedt@telekom.de), Deutsche Telekom

Justin Richer (jricher@mitre.org), MITRE

Nat Sakimura (n-sakimura@nri.co.jp), Nomura Research Institute, Ltd.

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

### Appendix B.  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 C.  Document History

[[ To be removed from the approved errata ]]

-29

* Referenced completed RFCs.
* Added missing URLs in references.
* Fixed issue #971 - Clarified default \*\_encrypted\_response\_enc and request\_object\_encryption\_enc values.
* Changed to use "Cache-Control: no-cache, no-store" and "Pragma: no-cache" in examples.
* Tracked terminology changes made in the referenced IETF specs since errata set 1.
* Updated the RFC 2616 reference to RFC 7231.
* Registered the client metadata definitions and token endpoint authentication methods not registered by RFC 7591 in the registries established by RFC 7591.

-28

* Final specification incorporating errata set 1.

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

### Authors' Addresses

|  |  |
| --- | --- |
|  | Nat Sakimura |
|  | Nomura Research Institute, Ltd. |
| **Email:** | [n-sakimura@nri.co.jp](mailto:n-sakimura@nri.co.jp) |
| **URI:** | <http://nat.sakimura.org/> |
|  |  |
|  | John Bradley |
|  | Ping Identity |
| **Email:** | [ve7jtb@ve7jtb.com](mailto:ve7jtb@ve7jtb.com) |
| **URI:** | <http://www.thread-safe.com/> |
|  |  |
|  | Michael B. Jones |
|  | Microsoft |
| **Email:** | [mbj@microsoft.com](mailto:mbj@microsoft.com) |
| **URI:** | <http://self-issued.info/> |