International Standard

ISO/IEC 26133

Information technology — OpenID connect — OpenID connect dynamic client registration 1.0 incorporating errata set 2

First edition
2024-10

Reference number
ISO/IEC 26133:2024(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 OpenID Connect Dynamic Client Registration 1.0 incorporating errata set 2) 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

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

Information technology — OpenID Connect — OpenID Connect Dynamic Client Registration 1.0 incorporating errata set 2

1. Introduction

TOC

OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 [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 specification describes how an RP can register with an OP, and how registration information for the RP can be retrieved.

The previous versions of this specification are:

- OpenID Connect Registration 1.0 incorporating errata set 1 [OpenID.Registration.Errata1]
- OpenID Connect Registration 1.0 (final) [OpenID.Registration.Final]

1.1. Requirements Notation and Conventions

TOC

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 [RFC2119].

In the .txt version of this specification, 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 specification, values to be taken literally are indicated by the use of `this fixed-width font`.

All uses of JSON Web Signature (JWS) [JWS] and JSON Web Encryption (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.

1.2. Terminology

TOC

This specification uses the terms "Access Token", "Authorization Code", "Authorization Endpoint", "Authorization Server", "Client", "Client Authentication", "Client Identifier", "Client Secret", "Grant Type", "Protected Resource", "Redirection URI", "Refresh Token", "Response Type", and "Token Endpoint" defined by OAuth 2.0 [RFC6749], the terms "JSON Web Token (JWT)" and "Nested JWT" defined by JSON Web Token (JWT) [JWT], the term "Base64url Encoding" defined by JSON Web Signature (JWS) [JWS], and the terms defined by OpenID Connect Core 1.0 [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.

---

2. Client Metadata

TOC

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] (Simple String Comparison).

response_types

OPTIONAL. JSON [RFC8259] 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`
- `id_token token`: `implicit`
- `code id_token`: `authorization_code`, `implicit`
- `code token`: `authorization_code`, `implicit`
- `code id_token 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 loopback URLs using the `http` scheme; loopback URLs use `localhost` or the IP loopback literals `127.0.0.1` or `[::1]` 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 loopback 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.

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.

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.

policy_uri

OPTIONAL. URL that the Relying Party Client provides to the End-User to read about 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.

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