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/IEC 2024



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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.

© ISO/IEC 2024 – All rights reserved

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.

© ISO/IEC 2024 – All rights reserved

Table of Contents

1. Introduction
1.1. Requirements Notation and Conventions
1.2. Terminology
2. Client Metadata
2.1. Metadata Languages and Scripts
3. Client Registration Endpoint
3.1. Client Registration Request
3.2. Client Registration Response
3.3. Client Registration Error Response
4. Client Configuration Endpoint
4.1. Forming the Client Configuration Endpoint URL
4.2. Client Read Request
4.3. Client Read Response
4.4. Client Read Error Response
5. "sector_identifier_uri" Validation
6. String Operations
7. Validation
8. Implementation Considerations
8.1. Compatibility Notes
8.2. Implementation Notes on Stateless Dynamic Client Registration
9. Security Considerations
9.1. Impersonation
9.2. Native Code Leakage
9.3. TLS Requirements
10. IANA Considerations
10.1. OAuth Dynamic Client Registration Metadata Registration
10.1.1. Registry Contents
10.2. OAuth Token Endpoint Authentication Methods Registration
10.2.1. Registry Contents
11. References
11.1. Normative References
11.2. Informative References

© ISO/IEC 2024 – All rights reserved

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`.

© ISO/IEC 2024 – All rights reserved

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

© ISO/IEC 2024 – All rights reserved