

ISO/IEC 26131:2024-10 (E)

Information technology - OpenID connect - OpenID connect core 1.0 incorporating errata set 2

Contents	Page
<u>1.</u> Introduction	
<u>1.1.</u> Requirements Notation and Conventions	
<u>1.2.</u> Terminology	
<u>1.3.</u> Overview	
<u>2.</u> ID Token	
<u>3.</u> Authentication	
<u>3.1.</u> Authentication using the Authorization Code Flow	
<u>3.1.1.</u> Authorization Code Flow Steps	
<u>3.1.2.</u> Authorization Endpoint	
<u>3.1.2.1.</u> Authentication Request	
<u>3.1.2.2.</u> Authentication Request Validation	
<u>3.1.2.3.</u> Authorization Server Authenticates End-User	
<u>3.1.2.4.</u> Authorization Server Obtains End-User Consent/Authorization	
<u>3.1.2.5.</u> Successful Authentication Response	
<u>3.1.2.6.</u> Authentication Error Response	
<u>3.1.2.7.</u> Authentication Response Validation	
<u>3.1.3.</u> Token Endpoint	
<u>3.1.3.1.</u> Token Request	
<u>3.1.3.2.</u> Token Request Validation	
<u>3.1.3.3.</u> Successful Token Response	
<u>3.1.3.4.</u> Token Error Response	
<u>3.1.3.5.</u> Token Response Validation	
<u>3.1.3.6.</u> ID Token	
<u>3.1.3.7.</u> ID Token Validation	
<u>3.1.3.8.</u> Access Token Validation	
<u>3.2.</u> Authentication using the Implicit Flow	
<u>3.2.1.</u> Implicit Flow Steps	
<u>3.2.2.</u> Authorization Endpoint	
<u>3.2.2.1.</u> Authentication Request	
<u>3.2.2.2.</u> Authentication Request Validation	
<u>3.2.2.3.</u> Authorization Server Authenticates End-User	
<u>3.2.2.4.</u> Authorization Server Obtains End-User Consent/Authorization	
<u>3.2.2.5.</u> Successful Authentication Response	
<u>3.2.2.6.</u> Authentication Error Response	
<u>3.2.2.7.</u> Redirect URI Fragment Handling	
<u>3.2.2.8.</u> Authentication Response Validation	
<u>3.2.2.9.</u> Access Token Validation	
<u>3.2.2.10.</u> ID Token	
<u>3.2.2.11.</u> ID Token Validation	
<u>3.3.</u> Authentication using the Hybrid Flow	
<u>3.3.1.</u> Hybrid Flow Steps	
<u>3.3.2.</u> Authorization Endpoint	

- [3.3.2.1.](#) **Authentication Request**
- [3.3.2.2.](#) **Authentication Request Validation**
- [3.3.2.3.](#) **Authorization Server Authenticates End-User**
- [3.3.2.4.](#) **Authorization Server Obtains End-User Consent/Authorization**
- [3.3.2.5.](#) **Successful Authentication Response**
- [3.3.2.6.](#) **Authentication Error Response**
- [3.3.2.7.](#) **Redirect URI Fragment Handling**
- [3.3.2.8.](#) **Authentication Response Validation**
- [3.3.2.9.](#) **Access Token Validation**
- [3.3.2.10.](#) **Authorization Code Validation**
- [3.3.2.11.](#) **ID Token**
- [3.3.2.12.](#) **ID Token Validation**
- [3.3.3.](#) **Token Endpoint**
 - [3.3.3.1.](#) **Token Request**
 - [3.3.3.2.](#) **Token Request Validation**
 - [3.3.3.3.](#) **Successful Token Response**
 - [3.3.3.4.](#) **Token Error Response**
 - [3.3.3.5.](#) **Token Response Validation**
 - [3.3.3.6.](#) **ID Token**
 - [3.3.3.7.](#) **ID Token Validation**
 - [3.3.3.8.](#) **Access Token**
 - [3.3.3.9.](#) **Access Token Validation**
- [4.](#) **Initiating Login from a Third Party**
- [5.](#) **Claims**
 - [5.1.](#) **Standard Claims**
 - [5.1.1.](#) **Address Claim**
 - [5.1.2.](#) **Additional Claims**
 - [5.2.](#) **Claims Languages and Scripts**
 - [5.3.](#) **UserInfo Endpoint**
 - [5.3.1.](#) **UserInfo Request**
 - [5.3.2.](#) **Successful UserInfo Response**
 - [5.3.3.](#) **UserInfo Error Response**
 - [5.3.4.](#) **UserInfo Response Validation**
 - [5.4.](#) **Requesting Claims using Scope Values**
 - [5.5.](#) **Requesting Claims using the "claims" Request Parameter**
 - [5.5.1.](#) **Individual Claims Requests**
 - [5.5.1.1.](#) **Requesting the "acr" Claim**
 - [5.5.2.](#) **Languages and Scripts for Individual Claims**
 - [5.6.](#) **Claim Types**
 - [5.6.1.](#) **Normal Claims**
 - [5.6.2.](#) **Aggregated and Distributed Claims**
 - [5.6.2.1.](#) **Example of Aggregated Claims**
 - [5.6.2.2.](#) **Example of Distributed Claims**
 - [5.7.](#) **Claim Stability and Uniqueness**
- [6.](#) **Passing Request Parameters as JWTs**
 - [6.1.](#) **Passing a Request Object by Value**

- [6.1.1.](#) Request using the "request" Request Parameter
- [6.2.](#) Passing a Request Object by Reference
 - [6.2.1.](#) URI Referencing the Request Object
 - [6.2.2.](#) Request using the "request_uri" Request Parameter
 - [6.2.3.](#) Authorization Server Fetches Request Object
 - [6.2.4.](#) "request_uri" Rationale
- [6.3.](#) Validating JWT-Based Requests
 - [6.3.1.](#) Encrypted Request Object
 - [6.3.2.](#) Signed Request Object
 - [6.3.3.](#) Request Parameter Assembly and Validation
- [7.](#) Self-Issued OpenID Provider
 - [7.1.](#) Self-Issued OpenID Provider Discovery
 - [7.2.](#) Self-Issued OpenID Provider Registration
 - [7.2.1.](#) Providing Information with the "registration" Request Parameter
 - [7.3.](#) Self-Issued OpenID Provider Request
 - [7.4.](#) Self-Issued OpenID Provider Response
 - [7.5.](#) Self-Issued ID Token Validation
- [8.](#) Subject Identifier Types
 - [8.1.](#) Pairwise Identifier Algorithm
- [9.](#) Client Authentication
- [10.](#) Signatures and Encryption
 - [10.1.](#) Signing
 - [10.1.1.](#) Rotation of Asymmetric Signing Keys
 - [10.2.](#) Encryption
 - [10.2.1.](#) Rotation of Asymmetric Encryption Keys
- [11.](#) Offline Access
- [12.](#) Using Refresh Tokens
 - [12.1.](#) Refresh Request
 - [12.2.](#) Successful Refresh Response
 - [12.3.](#) Refresh Error Response
- [13.](#) Serializations
 - [13.1.](#) Query String Serialization
 - [13.2.](#) Form Serialization
 - [13.3.](#) JSON Serialization
- [14.](#) String Operations
- [15.](#) Implementation Considerations
 - [15.1.](#) Mandatory to Implement Features for All OpenID Providers
 - [15.2.](#) Mandatory to Implement Features for Dynamic OpenID Providers
 - [15.3.](#) Discovery and Registration
 - [15.4.](#) Mandatory to Implement Features for Relying Parties
 - [15.5.](#) Implementation Notes
 - [15.5.1.](#) Authorization Code Implementation Notes

- [15.5.2.](#) **Nonce Implementation Notes**
 - [15.5.3.](#) **Redirect URI Fragment Handling**
- Implementation Notes**
- [15.6.](#) **Compatibility Notes**
 - [15.7.](#) **Related Specifications and Implementer's Guides**
- 16. Security Considerations**
- [16.1.](#) **Request Disclosure**
 - [16.2.](#) **Server Masquerading**
 - [16.3.](#) **Token Manufacture/Modification**
 - [16.4.](#) **Access Token Disclosure**
 - [16.5.](#) **Server Response Disclosure**
 - [16.6.](#) **Server Response Repudiation**
 - [16.7.](#) **Request Repudiation**
 - [16.8.](#) **Access Token Redirect**
 - [16.9.](#) **Token Reuse**
 - [16.10.](#) **Eavesdropping or Leaking Authorization Codes (Secondary Authenticator Capture)**
 - [16.11.](#) **Token Substitution**
 - [16.12.](#) **Timing Attack**
 - [16.13.](#) **Other Crypto Related Attacks**
 - [16.14.](#) **Signing and Encryption Order**
 - [16.15.](#) **Issuer Identifier**
 - [16.16.](#) **Implicit Flow Threats**
 - [16.17.](#) **TLS Requirements**
 - [16.18.](#) **Lifetimes of Access Tokens and Refresh**
- Tokens**
- [16.19.](#) **Symmetric Key Entropy**
 - [16.20.](#) **Need for Signed Requests**
 - [16.21.](#) **Need for Encrypted Requests**
 - [16.22.](#) **HTTP 307 Redirects**
 - [16.23.](#) **Custom URI Schemes on iOS**
- 17. Privacy Considerations**
- [17.1.](#) **Personally Identifiable Information**
 - [17.2.](#) **Data Access Monitoring**
 - [17.3.](#) **Correlation**
 - [17.4.](#) **Offline Access**
- 18. IANA Considerations**
- [18.1.](#) **JSON Web Token Claims Registration**
 - [18.1.1.](#) **Registry Contents**
 - [18.2.](#) **OAuth Parameters Registration**
 - [18.2.1.](#) **Registry Contents**
 - [18.3.](#) **OAuth Extensions Error Registration**
 - [18.3.1.](#) **Registry Contents**
 - [18.4.](#) **URI Scheme Registration**
 - [18.4.1.](#) **Registry Contents**
- 19. References**
- [19.1.](#) **Normative References**
 - [19.2.](#) **Informative References**

Appendix A. **Authorization Examples**

- A.1. **Example using response_type=code**
- A.2. **Example using response_type=id_token**
- A.3. **Example using response_type=id_token token**
- A.4. **Example using response_type=code id_token**
- A.5. **Example using response_type=code token**
- A.6. **Example using
response_type=code id_token token**
- A.7. **RSA Key Used in Examples**