OAuth Working Group
Internet-Draft
Updates: 7521, 7522, 7523, 9126 (if approved)
Intended status: Standards Track
Expires: 23 January 2026

M.B. Jones
Self-Issued Consulting
B. Campbell
Ping Identity
C. Mortimore
Disney
F. Skokan
Okta

22 July 2025

Updates to Audience Values for OAuth 2.0 Authorization Servers
draft-ietf-oauth-rfc7523bis-02

Abstract

This specification updates the requirements for audience values for tokens whose audience is an OAuth 2.0 authorization server to address a security vulnerability identified in the previous requirements for those audience values in multiple OAuth 2.0 specifications.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 23 January 2026.

Copyright Notice

Table of Contents

1. Introduction

Multiple OAuth 2.0 specifications use tokens (also known as "assertions") that are sent to authorization servers. These tokens contain an audience value or values intended to identify the recipients that the token is intended for. When the token is a JSON Web Token (JWT) [JWT], the audience value(s) are contained in the aud (audience) claim.

When performing a security analysis of a pre-final version of the OpenID Federation specification [OpenID.Federation], University of Stuttgart security researchers Pedram Hosseyni, Dr. Ralf K端sters, and Tim W端rtele discovered a vulnerability affecting multiple OpenID and OAuth specifications caused by ambiguities in the audience values of tokens sent to authorization servers. The vulnerability was disclosed to the OAuth working group in an interim meeting in January 2025 called for that purpose, including providing a description of the vulnerability [private_key_jwt.Disclosure]. A paper they published describing the attack is [Audience.Injection].

This specification updates the affected OAuth specifications to address the security vulnerability identified. Specifically, it eliminates former ambiguities in the audience values of tokens sent to OAuth 2.0 authorization servers.

A general description of the update made to each specification is for it to require that the issuer identifier URL of the authorization server, as defined in [RFC8414], be used as the sole value of the token audience. Furthermore, the authorization server MUST reject any such token that does not contain its own issuer identifier as the sole audience value. An explicit type for each affected kind of token, as defined in [RFC8725], is also defined to facilitate distinguishing between tokens produced in accordance with specifications published prior to these updates and those incorporating them. Specific updates made to each affected specification follow.

1.1. Notational 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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.2. Terminology

All terms are as defined in the following specifications: "The OAuth 2.0 Authorization Framework" [RFC6749], "Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants" [RFC7521], and "JSON Web Token (JWT)" [JWT].

2. Updates to RFC 7521

This section updates "Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants" [RFC7521] to tighten its audience requirements.

The description of the Audience parameter in Section 5.1 of [RFC7521] (Assertion Metamodel) is replaced by:

Audience
: A value that identifies the party intended to process the assertion. The audience value MUST identify the authorization server as the intended audience. It is the responsibility of the client to use only audience values that are specific to the authorization server being used. This MAY be the issuer identifier of the authorization server. The authorization server MUST reject any assertion that does not contain its own identity as the intended audience.

The description of the Audience parameter in Section 5.2 of [RFC7521] (General Assertion Format and Processing Rules) is replaced by:

> The assertion MUST contain an audience value that identifies the authorization server as the intended audience. It is the responsibility of the client to use only audience values that are specific to the authorization server being used. The authorization server MUST reject any assertion that does not contain its own identity as the intended audience.

3. Updates to RFC 7522

This section updates "Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants" [RFC7522]. It tightens its audience requirements for SAML authorization grants and it deprecates the use of SAML assertions for client authentication.

The text and example in Section 2.2 of [RFC7522] (Using SAML Assertions for Client Authentication) is replaced by:

> It is RECOMMENDED that SAML Bearer Assertions not be used for for client authentication.

The description of the Audience element in Item 2 of Section 3 of [RFC7522] (Assertion Format and Processing Requirements) is replaced by:

> The Assertion MUST contain a <Conditions> element with an <AudienceRestriction> element with an <Audience> element that identifies the authorization server as the intended audience. It is the responsibility of the client to use only audience values that are specific to the authorization server being used. This MAY be the issuer identifier of the authorization server, the token endpoint URL of the authorization server, or a SAML Entity ID. Section 2.5.1.4 of "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0" [OASIS.saml-core-2.0-os] defines the <AudienceRestriction> and

> <Audience> elements. The authorization server MUST reject any assertion that does not contain its own identity as the intended audience.

In Section 4 of [RFC7522] (Authorization Grant Example), the sentence:

> The intended audience of the Assertion is https://saml-sp.example.net, which is an identifier for a SAML Service Provider with which the authorization server identifies itself.

is replaced by:

> The intended audience of the Assertion is https://authz.example.net, which is the authorization server’s issuer identifier.

In the same section, the SAML 2.0 Assertion example is replaced by:

```
<Assertion IssueInstant="2025-07-17T00:53:34.619Z"
  ID="ef1xsbZxPV2oqjd7HTLRLIBlBb7"
  Version="2.0"
  xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
 <Issuer>https://saml-idp.example.com</Issuer>
 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  [...omitted for brevity...]
 </ds:Signature>
 <Subject>
  <NameID
   Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">
   brian@example.com
  </NameID>
  <SubjectConfirmation
    Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
   <SubjectConfirmationData
     NotOnOrAfter="2025-07-17T00:58:34.619Z"
     Recipient="https://authz.example.net/token.oauth2"/>
   </SubjectConfirmation>
  </Subject>
  <Conditions>
    <AudienceRestriction>
      <Audience>https://authz.example.net</Audience>
    </AudienceRestriction>
  </Conditions>
  <AuthnStatement AuthnInstant="2025-07-17T00:53:34.371Z">
    <AuthnContext>
      <AuthnContextClassRef>
        urn:oasis:names:tc:SAML:2.0:ac:classes:X509
      </AuthnContextClassRef>
    </AuthnContext>
  </AuthnStatement>
</Assertion>
```

Figure 1: Example SAML 2.0 Assertion

4. Updates to RFC 7523

This section updates "JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants" [RFC7523] to tighten its audience requirements.

In Section 2.2 of [RFC7523] (Using JWTs for Client Authentication), the example is replaced by:

```
POST /token.oauth2 HTTP/1.1
Host: as.example.com
Content-Type: application/x-www-form-urlencoded

grant_type=authorization_code&
code=n0esc3NRze7LTCu7iYzS6a5acc3f0ogp4&
client_assertion_type=urn%3Aietf%3Aparams%3Aoauth%3A
  client-assertion-type%3Ajwt-bearer&
client_assertion=eyJ0eXAiOiJjbGllbnQtYXV0aGVudGljYXRpb24rand0IiwiYWx
  nIjoiRVMyNTYiLCJraWQiOiIxNiJ9.
e2F1ZDpodHRwczovL2F1dGh6LmV4YW1wbGUubmV0LA[...omitted...].
cC4hiUPo[...omitted for brevity...]
```

In Section 3 of [RFC7523] (JWT Format and Processing Requirements), Item 3, which describes the audience value, is replaced by:

> The JWT MUST contain an aud (audience) claim containing a value that identifies the authorization server as the intended audience. Two cases are differentiated:
>
> a. For the authorization grant, it is the responsibility of the client to use only audience values that are specific to the authorization server being used. This MAY be either the issuer identifier of the authorization server or the token endpoint URL of the authorization server. The authorization server MUST reject any JWT that does not contain its own identity as the intended audience, and if the value of aud is an array, all array values MUST identify the authorization server as the intended audience.
>
> b. For client authentication, the aud (audience) claim value MUST use the issuer identifier [RFC8414] of the authorization server as its sole value. The authorization server MUST have an issuer identifier to be used with this specification. Unlike the aud value specified in [RFC7523], there MUST be no value other than the issuer identifier of the intended authorization server used as the audience of the JWT; this includes that the token endpoint URL of the authorization server MUST NOT be used as an audience value. To simplify implementations, the aud claim value MUST be a JSON string, and not a single-valued JSON array. The authorization server MUST reject any JWT that does not contain its issuer identifier as its sole audience value.
>
> In the absence of an application profile specifying otherwise, applications MUST compare the audience values using the Simple String Comparison method defined in Section 6.2.1 of RFC 3986 [RFC3986].

In Section 3.2 of [RFC7523] (Client Authentication Processing), the following requirement is added:

> Client authentication JWTs MUST be explicitly typed by using the typ header parameter value client-authentication+jwt another more specific explicit type value defined by a specification profiling this specification. Client authentication JWTs not using the explicit type value MUST be rejected by the authorization server.

In Section 4 of [RFC7523] (Authorization Grant Example), the sentence:

> The intended audience of the JWT is https://jwt-rp.example.net, which is an identifier with which the authorization server identifies itself.

is replaced by:

> The intended audience of the JWT is https://authz.example.net, which is the authorization server’s issuer identifier.

In the same section, the JWT Claims Set example is replaced by:

```
{"aud":"https://authz.example.net",
 "iss":"https://jwt-idp.example.com",
 "sub":"mailto:mike@example.com",
 "iat":1731721541,
 "exp":1731725141,
 "http://claims.example.com/member":true
}
```

Figure 2: Example JWT Claims Set

In the list of agreements required by participants in Section 5 of [RFC7523] (Interoperability Considerations), an agreement on "audience identifiers" is no longer needed for client authentication JWTs.

The additional example in the following subsection is added after Section 4 of [RFC7523]

4.1. Client Authentication JWT Example

The following example illustrates what a client authentication JWT and token request using it would look like.

The example shows a JWT issued and signed by the system entity identified as https://jwt-idp.example.com. The subject of the JWT is identified by email address as mike@example.com. The intended audience of the JWT is https://authz.example.net, which is the authorization server's issuer identifier. The JWT is sent as part of a token request to the authorization server's token endpoint at https://authz.example.net/token.oauth2.

Below is an example JSON object that could be encoded to produce the JWT Claims Set for a client authentication JWT:

```
{"aud":"https://authz.example.net",
 "iss":"https://jwt-idp.example.com",
 "sub":"mailto:mike@example.com",
 "iat":1752702206,
 "exp":1752705806,
 "http://claims.example.com/member":true
}
```

The following example JSON object, used as the header parameters of a JWT, declares that the JWT is a client authentication JWT, is signed with the Elliptic Curve Digital Signature Algorithm (ECDSA) P-256 with SHA-256, and was signed with a key identified by the kid value 16.

```
{"typ":"client-authentication+jwt","alg":"ES256","kid":"16"}
```

To present the JWT with the claims and header parameters shown above as part of an access token request, for example, the client might make the following HTTPS request (with extra line breaks for display purposes only):

```
POST /token.oauth2 HTTP/1.1
Host: authz.example.net
Content-Type: application/x-www-form-urlencoded

grant_type=authorization_code&
code=n0esc3NRze7LTCu7iYzS6a5acc3f0ogp4&
client_assertion_type=urn%3Aietf%3Aparams%3Aoauth%3A
  client-assertion-type%3Ajwt-bearer&
client_assertion=eyJ0eXAiOiJjbGllbnQtYXV0aGVudGljYXRpb24rand0IiwiYWx
  nIjoiRVMyNTYiLCJraWQiOiIxNiJ9.
e2F1ZDpodHRwczovL2F1dGh6LmV4YW1wbGUubmV0LA[...omitted...].
J9l-ZhwP[...omitted for brevity...]
```

5. Updates to RFC 9126

This section updates "OAuth 2.0 Pushed Authorization Requests" [RFC9126] to tighten its audience requirements.

The paragraph describing the audience value in Section 2 of [RFC9126] (Pushed Authorization Request Endpoint) is replaced by:

> This update resolves the potential ambiguity regarding the appropriate audience value to use when employing JWT client assertion-based authentication (as defined in Section 2.2 of [RFC7523] and as updated by Section 4 with the private_key_jwt or client_secret_jwt authentication method names per Section 9 of [OpenID.Core]) that was described in [RFC9126]. To address that ambiguity, the issuer identifier URL of the authorization server according to [RFC8414] MUST be used as the sole value of the audience. The authorization server MUST reject any such JWT that does not contain its own issuer identifier as the sole audience value.

6. Security Considerations

The security considerations described within the following specifications are all applicable to this document: "Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants" [RFC7521], "Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants" [RFC7522], "JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants" [RFC7523], "OAuth 2.0 Pushed Authorization Requests" [RFC9126], "The OAuth 2.0 Authorization Framework" [RFC6749], and "JSON Web Token (JWT)" [JWT].

This specification tightens token audience requirements to prevent attacks that could result from exploiting audience ambiguities previously allowed by [RFC7521], [RFC7522], [RFC7523], and [RFC9126]. These attacks are described in [private_key_jwt.Disclosure] and [Audience.Injection].

7. IANA Considerations

7.1. Media Type Registration

This section registers the following media type [RFC2046] in the "Media Types" registry [IANA.MediaTypes] in the manner described in [RFC6838].

7.1.1. Registry Contents

* Type name: application
* Subtype name: client-authentication+jwt
* Required parameters: n/a
* Optional parameters: n/a
* Encoding considerations: binary; A client authentication JWT is a JWT; JWT values are encoded as a series of base64url-encoded values (some of which may be the empty string) separated by period ('.') characters.
* Security considerations: See Section 6 of this specification
* Interoperability considerations: n/a
* Published specification: Section 4 of this specification
* Applications that use this media type: Applications that use this specification
* Fragment identifier considerations: n/a
* Additional information:
  Magic number(s): n/a
  File extension(s): n/a
  Macintosh file type code(s): n/a
* Person & email address to contact for further information: Michael B. Jones, michael_b_jones@hotmail.com
* Intended usage: COMMON
* Restrictions on usage: none
* Author: Michael B. Jones, michael_b_jones@hotmail.com
* Change controller: IETF
* Provisional registration? No

8. References

8.1. Normative References

[JWT] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <https://www.rfc-editor.org/info/rfc7519>.

[OASIS.saml-core-2.0-os] Cantor, S., Kemp, J., Philpott, R., and E. Maler, "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0", OASIS Standard saml-core-2.0-os, March 2005, <https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <https://www.rfc-editor.org/info/rfc3986>.

[RFC6749] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework", RFC 6749, DOI 10.17487/RFC6749, October 2012, <https://www.rfc-editor.org/info/rfc6749>.

[RFC7521] Campbell, B., Mortimore, C., Jones, M., and Y. Goland, "Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants", RFC 7521, DOI 10.17487/RFC7521, May 2015, <https://www.rfc-editor.org/info/rfc7521>.

[RFC7522] Campbell, B., Mortimore, C., and M. Jones, "Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants", RFC 7522, DOI 10.17487/RFC7522, May 2015, <https://www.rfc-editor.org/info/rfc7522>.

[RFC7523] Jones, M., Campbell, B., and C. Mortimore, "JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants", RFC 7523, DOI 10.17487/RFC7523, May 2015, <https://www.rfc-editor.org/info/rfc7523>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8414] Jones, M., Sakimura, N., and J. Bradley, "OAuth 2.0 Authorization Server Metadata", RFC 8414, DOI 10.17487/RFC8414, June 2018, <https://www.rfc-editor.org/info/rfc8414>.

[RFC8725] Sheffer, Y., Hardt, D., and M. Jones, "JSON Web Token Best Current Practices", BCP 225, RFC 8725, DOI 10.17487/RFC8725, February 2020, <https://www.rfc-editor.org/info/rfc8725>.

[RFC9126] Lodderstedt, T., Campbell, B., Sakimura, N., Tonge, D., and F. Skokan, "OAuth 2.0 Pushed Authorization Requests", RFC 9126, DOI 10.17487/RFC9126, September 2021, <https://www.rfc-editor.org/info/rfc9126>.

8.2. Informative References

[Audience.Injection]
Hosseyni, P., K端sters, R., and T. W端rtele, "Audience Injection Attacks: A New Class of Attacks on Web-Based Authorization and Authentication Standards", Cryptology ePrint Archive Paper 2025/629, April 2025, <https://eprint.iacr.org/2025/629>.

[IANA.MediaTypes]
IANA, "Media Types", <https://www.iana.org/assignments/media-types>.

[OpenID.Core]
Sakimura, N., Bradley, J., Jones, M.B., de Medeiros, B., and C. Mortimore, "OpenID Connect Core 1.0 incorporating errata set 2", 15 December 2023, <https://openid.net/specs/openid-connect-core-1_0.html>.

[OpenID.Federation]
Hedberg, R., Jones, M. B., Solberg, A., Bradley, J., Marco, G. D., and V. Dzhuvinov, "OpenID Federation 1.0", 2 June 2025, <https://openid.net/specs/openid-federation-1_0.html>.

[private_key_jwt.Disclosure]
OpenID Foundation, "OIDF Responsible Disclosure Notice on Security Vulnerability for private_key_jwt", 24 January 2025, <https://openid.net/wp-content/uploads/2025/01/OIDF-Responsible-Disclosure-Notice-on-Security-Vulnerability-for-private_key_jwt.pdf>.

[RFC2046]
Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", RFC 2046, DOI 10.17487/RFC2046, November 1996, <https://www.rfc-editor.org/info/rfc2046>.

[RFC6838]
Freed, N., Klensin, J., and T. Hansen, "Media Type Specifications and Registration Procedures", BCP 13, RFC 6838, DOI 10.17487/RFC6838, January 2013, <https://www.rfc-editor.org/info/rfc6838>.

Appendix A. Document History

[[to be removed by the RFC Editor before publication as an RFC]]

-02

* Added Filip Skokan as an author.

* Applied Brian Campbell's suggestions made at IETF 122. Specifically:
  - Focused RFC 7523 updates on JWT client authentication case.
  - Described client responsibilities for the audience value of authorization grants. No longer mandate that the audience for authorization grants be the issuer identifier, so as to make a minimum of breaking changes.
  - Deprecated the use of SAML assertions for client authentication.

-01

* Reworked to make updates to RFC 7523, rather than replacing it.
* Removed updates to RFC 9101.
* Added reference to the University of Stuttgart paper [Audience.Injection].

-00

* Initial working group draft, replacing draft-jones-oauth-rfc7523bis-00.

Acknowledgements

We would like to acknowledge the contributions of the following people to this specification: John Bradley, Ralph Bragg, Joseph Heenan, Pedram Hosseyni, Aaron Parecki, and Tim W端rtele.

Authors' Addresses

Michael B. Jones
Self-Issued Consulting
Email: michael_b_jones@hotmail.com
URI: https://self-issued.info/

Brian Campbell
Ping Identity
Email: bcampbell@pingidentity.com

Chuck Mortimore
Disney

Email: charliemortimore@gmail.com

Filip Skokan
Okta
Email: panva.ip@gmail.com