Stream:	Internet Engineering Task Force (IETF)			
RFC:	10070			
Updates:	7521, 7522, 7523, 9126			
Category:	Standards Track			
Published:	November 2026			
ISSN:	2070-1721			
Authors:	M.B. Jones	B. Campbell	C. Mortimore	F. Skokan
	Self-Issued Consulting	*Ping Identity*	*Ticketmaster*	*Okta*

RFC 10070
Updates to OAuth 2.0 JSON Web Token (JWT) Client Authentication and Assertion-Based Authorization Grants

Abstract

This document updates RFCs 7521, 7522, 7523, and 9126 with respect to the treatment of audience values in OAuth 2.0 Client Assertion Authentication and Assertion-based Authorization Grants 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 is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc10070.

Copyright Notice

Copyright (c) 2026 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions

with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction 3
1.1. Notational Conventions 3
1.2. Terminology 3
2. Updates to RFC 7521 4
3. Updates to RFC 7522 4
4. Updates to RFC 7523 6
4.1. Client Authentication JWT Example 9
5. Updates to RFC 9126 10
6. Operational Considerations 11
7. Security Considerations 11
8. IANA Considerations 12
8.1. Media Type Registration 12
8.1.1. Registry Contents 12
8.2. OAuth Token Endpoint Authentication Methods 13
8.2.1. Registry Contents 13
8.3. OAuth URI Registration Updates 13
9. References 13
9.1. Normative References 13
9.2. Informative References 14
Acknowledgements 15
Authors' Addresses 15

1. Introduction

Multiple OAuth 2.0 specifications use tokens (also known as "assertions") that are sent to authorization servers. These tokens contain audience value(s) that identify the intended recipient(s). When the token is a JSON Web Token (JWT) [RFC7519], 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 Küsters, and Tim Würtele 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 and a description of the vulnerability [private_key_jwt.Disclosure] was provided. A paper they published describing the attack is [Audience.Injection].

This specification updates the affected OAuth specifications to address the security vulnerability that was identified. Specifically, it eliminates former choices in the audience values of tokens sent to OAuth 2.0 authorization servers. Section 3.3 of [RFC8414] requires that the client having retrieved the metadata validates the returned issuer value. Other endpoint values of the metadata cannot be directly validated and, if used as the audience when sent to a different endpoint, can open an attack vector.

A general description of the updates made is to require that the issuer identifier URL of the authorization server, as defined in [RFC8414], be used as the sole value of the audience of the JWT client authentication assertion. Furthermore, the authorization server rejects any JWT client authentication assertion that does not contain its own issuer identifier as the sole audience value. An explicit type for the JWT client authentication assertion, 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)" [RFC7519].

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 as follows.

OLD:

> Audience
> A value that identifies the party or parties intended to process the assertion. The URL of the token endpoint, as defined in Section 3.2 of OAuth 2.0 [RFC6749], can be used to indicate that the authorization server is a valid intended audience of the assertion. In the absence of an application profile specifying otherwise, compliant applications MUST compare the Audience values using the Simple String Comparison method defined in Section 6.2.1 of RFC 3986 [RFC3986].

NEW:

> Audience
> A value that identifies the party intended to process the assertion. The issuer identifier of the authorization server, as defined in [RFC8414], can be used to indicate that the authorization server is a valid intended audience of the assertion.

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 as follows.

OLD:

> To use a SAML Bearer Assertion for client authentication, the client uses the following parameter values and encodings.
>
> The value of the "client_assertion_type" parameter is "urn:ietf:params:oauth:client-assertion-type:saml2-bearer".
>
> The value of the "client_assertion" parameter MUST contain a single SAML 2.0 Assertion. The SAML Assertion XML data MUST be encoded using base64url, where the encoding adheres to the definition in Section 5 of RFC 4648 [RFC4648] and where the padding bits are set to zero. To avoid the need for subsequent encoding steps (by "application/x-www-form-urlencoded" [W3C.REC-html401-19991224], for example), the base64url-encoded data SHOULD NOT be line wrapped and pad characters ("=") SHOULD NOT be included.
>
> The following example demonstrates a client authenticating using an Assertion during the presentation of an authorization code grant in an access token request (with extra line breaks for display purposes only):
>
> ```
> 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
> %3Aclient-assertion-type%3Asaml2-bearer&
> client_assertion=PHNhbW...[omitted for brevity]...ZT
> ```

NEW:

> SAML Bearer Assertions **MUST NOT** be used for client authentication for any new applications. Should any applications already be doing this in the manner described in Section 2.2 of [RFC7522], it is left to the discretion of their implementers and deployers whether to migrate away from this feature and/or potentially tighten the audience values used in a manner parallel to the changes being made to RFC 7523 by this specification.

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

OLD:

> The Assertion **MUST** contain a <Conditions> element with an <AudienceRestriction> element with an <Audience> element that identifies the authorization server as an intended audience. 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 and, in addition to the URI references discussed there, the token endpoint URL of the authorization server MAY be used as a URI that identifies the authorization server as an intended audience. The authorization server MUST reject any Assertion that does not contain its own identity as the intended audience. In the absence of an application profile specifying otherwise, compliant applications MUST compare the Audience values using the Simple String Comparison method defined in Section 6.2.1 of RFC 3986 [RFC3986]. As noted in Section 5, the precise strings to be used as the Audience for a given authorization server must be configured out of band by the authorization server and the issuer of the Assertion.

NEW:

> The Assertion **MUST** contain a <Conditions> element with an <AudienceRestriction> element with an <Audience> element that identifies the authorization server as the intended audience. The client is responsible for ensuring that the audience of the Assertion is appropriate for the authorization server to which it is sent. 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.

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 3 of [RFC7523] (JWT Format and Processing Requirements), Item 3, which describes the audience value, is replaced as follows.

OLD:

> The JWT **MUST** contain an "aud" (audience) claim containing a value that identifies the authorization server as an intended audience. The token endpoint URL of the authorization server **MAY** be used as a value for an "aud" element to identify the authorization server as an intended audience of the JWT. The authorization server **MUST** reject any JWT that does not contain its own identity as the intended audience. In the

absence of an application profile specifying otherwise, compliant applications **MUST** compare the audience values using the Simple String Comparison method defined in Section 6.2.1 of RFC 3986 [RFC3986]. As noted in Section 5, the precise strings to be used as the audience for a given authorization server must be configured out of band by the authorization server and the issuer of the JWT.

NEW:

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, the client is responsible for ensuring that the audience of the JWT assertion is appropriate for the authorization server to which it is sent. An authorization server **MAY** be identified by either its issuer identifier or its token endpoint URL.
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. The "aud" claim value **MUST** indicate only the issuer identifier of the intended authorization server 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. 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 [RFC3986].

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

Client authentication JWTs **SHOULD** be explicitly typed by using the "typ" header parameter value "client-authentication+jwt" or another more specific explicit type value defined by a specification profiling this specification.

The introduction of strong typing for JWTs (using explicit "typ" values) serves as a signal to distinguish between tokens produced in accordance with specifications published prior to these updates and those incorporating them. However, the primary security protection comes from the tightened audience requirements. The use of explicit typing enables clients to signal their compliance with the requirements herein. However, since strong typing alone does not prevent the attacks described in [private_key_jwt.Disclosure] and [Audience.Injection], it is **NOT RECOMMENDED** for servers to reject JWTs that do not have explicit types. Such rejection would cause

> interoperability issues with clients that already conform to the tightened audience requirements but have not yet adopted explicit typing. This approach balances security signaling with practical deployment considerations, avoiding disruption to client deployments that already conform to the tightened audience requirements but have not yet adopted explicit typing.

In Section 4 of [RFC7523] (Authorization Grant Example), the sentence below is replaced as follows.

OLD:

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

NEW:

> 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 as follows.

OLD:

```
{"iss":"https://jwt-idp.example.com",
 "sub":"mailto:mike@example.com",
 "aud":"https://jwt-rp.example.net",
 "nbf":1300815780,
 "exp":1300819380,
 "http://claims.example.com/member":true}
```

NEW:

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

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 OAuth client identified as "https://client.example". 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:

```
{
  "iss": "https://client.example",
  "sub": "https://client.example",
  "aud": "https://authz.example.net",
  "iat": 1752702206,
  "exp": 1752705806
}
```

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.eyJhdWQiOiJodHRwczovL2F1dGh6LmV4YW1w
  bGUubmV0IiwiaXNzIjoiaHR0cHM6Ly9jbGllbnQuZXhhbXBsZSIsInN1YiI6Imh0dH
  BzOi8vY2xpZW50LmV4YW1wbGUiLCJpYXQiOjE3NTI3MDIyMDYsImV4cCI6MTc1Mjcw
  NTgwNn0.6KrSQUxdl9ehs[...omitted for brevity...]bwc0ZOJw
```

5. Updates to RFC 9126

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

The last paragraph in Section 2 of [RFC9126] (Pushed Authorization Request Endpoint), which describes the audience value, is replaced as follows.

OLD:

> Due to historical reasons, there is potential ambiguity regarding the appropriate audience value to use when employing JWT client assertion-based authentication (defined in Section 2.2 of [RFC7523] with private_key_jwt or client_secret_jwt authentication method names per Section 9 of [OpenID.Core]). To address that ambiguity, the issuer identifier URL of the authorization server according to [RFC8414] SHOULD be used as the value of the audience. In order to facilitate interoperability, the authorization server MUST accept its issuer identifier, token endpoint URL, or pushed authorization request endpoint URL as values that identify it as an intended audience.

NEW:

Due to historical reasons, there is 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]). 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.

Client authentication JWTs **SHOULD** be explicitly typed by using the "typ" header parameter value "client-authentication+jwt" or another more specific explicit type value defined by a specification profiling this specification.

The introduction of strong typing for JWTs (using explicit "typ" values) serves as a signal to distinguish between tokens produced in accordance with specifications published prior to these updates and those incorporating them. However, the primary security protection comes from the tightened audience requirements. The use of explicit typing enables clients to signal their compliance with the requirements herein. However, since strong typing alone does not prevent the attacks described in [private_key_jwt.Disclosure] and [Audience.Injection], it is **NOT RECOMMENDED** for servers to reject JWTs that do not have explicit types. Such rejection would cause interoperability issues with clients that already conform to the tightened audience requirements but have not yet adopted explicit typing. This approach balances security signaling with practical deployment considerations, avoiding disruption to client deployments that already conform to the tightened audience requirements but have not yet adopted explicit typing.

6. Operational Considerations

Changes in this specification affect interoperability between clients and authorization servers that implement different versions. In particular, the resulting compatibility is not entirely symmetric. A client implementing this specification will interoperate with both authorization servers conforming to the updates herein as well as authorization servers implementing earlier versions. However, some clients implementing earlier versions may not interoperate with authorization servers that strictly enforce the updated requirements in this specification. Deployments upgrading to this specification should consider this asymmetry when planning rollouts or migrations, as it may be necessary to ensure that clients are updated before, or in coordination with, authorization servers that enforce the updated behavior.

7. 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)" [RFC7519].

This specification tightens treatment of assertion audience values 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].

8. IANA Considerations

8.1. Media Type Registration

IANA has registered the following media type [RFC2046] in the "Media Types" registry [IANA.MediaTypes] in the manner described in [RFC6838].

8.1.1. 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 7 of RFC 10070

Interoperability considerations: N/A

Published specification: Section 4 of RFC 10070

Applications that use this media type: Applications that use RFC 10070

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: IETF OAuth Working Group <oauth@ietf.org>

Intended usage: COMMON

Restrictions on usage: none

Author: Michael B. Jones <michael_b_jones@hotmail.com>

Change controller: IETF

Provisional registration? No

8.2. OAuth Token Endpoint Authentication Methods

IANA has updated the following entries in the "OAuth Token Endpoint Authentication Methods" registry of [IANA.OAuthParameters].

8.2.1. Registry Contents

Token Endpoint Authentication Method Name: private_key_jwt
Change Controller: IESG
Reference: Section 9 of [OpenID.Core], RFC 10070

Token Endpoint Authentication Method Name: client_secret_jwt
Change Controller: IESG
Reference: Section 9 of [OpenID.Core], RFC 10070

8.3. OAuth URI Registration Updates

IANA has updated the following entries in the "OAuth URI" registry of [IANA.OAuthParameters] to list RFC 10070 as an additional reference.

- urn:ietf:params:oauth:grant-type:jwt-bearer
- urn:ietf:params:oauth:client-assertion-type:jwt-bearer
- urn:ietf:params:oauth:grant-type:saml2-bearer
- urn:ietf:params:oauth:client-assertion-type:saml2-bearer

9. References

9.1. Normative References

[OASIS.saml-core-2.0-os] Cantor, S., Ed., Kemp, J., Ed., Philpott, R., Ed., and E. Maler, Ed., "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>.

[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>.

[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>.

[RFC7519] 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>.

[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>.

9.2. Informative References

[Audience.Injection] Hosseyni, P., Küsters, R., and T. Würtele, "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>.

[IANA.OAuthParameters] IANA, "OAuth Parameters", <https://www.iana.org/assignments/oauth-parameters>.

[OpenID.Federation] Hedberg, R., Ed., Jones, M. B., Solberg, A., Bradley, J., Marco, G. D., and V. Dzhuvinov, "OpenID Federation 1.0", 17 February 2026, <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>.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006, <https://www.rfc-editor.org/info/rfc4648>.

[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>.

[W3C.REC-html401-19991224] Ragget, D., Ed., Hors, A., Ed., and I. Jacobs, Ed., "HTML 4.01 Specification", World Wide Web Consortium Recommendation REC-html401-19991224, December 1999, <https://www.w3.org/TR/1999/REC-html401-19991224/>.

Acknowledgements

We would like to acknowledge the contributions of the following people to this specification: Brock Allen, John Bradley, Ralph Bragg, Deb Cooley, Jim Fenton, Mahesh Jethanandani, Joseph Heenan, Pedram Hosseyni, Luigi Iannone, Pieter Kasselman, Jamshid Khosravian, Ralf Küsters, Martin Lindström, Axel Nennker, Aaron Parecki, Rich Salz, Dean H. Saxe, Arndt Schwenkschuster, Rifaat Shekh-Yusef, and Tim Würtele.

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
Ticketmaster
Email: charliemortimore@gmail.com

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