Web Authorization Protocol
Internet-Draft
Updates: 7523, 7522, 7521, 9126 (if approved)
Intended status: Standards Track
Expires: 22 September 2025

M. B. Jones
Self-Issued Consulting
C. Mortimore
Disney
B. Campbell
Ping Identity
21 March 2025

Updates to OAuth 2.0 Client Asseertion Authentication and Assertion Based Authorization Grants
draft-campbell-oauth-rfc7523redux-00

Abstract

TODO Abstract

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://bc-pi.github.io/7523redux/draft-campbell-oauth-rfc7523redux.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-campbell-oauth-rfc7523redux/.

Discussion of this document takes place on the Web Authorization Protocol Working Group mailing list (mailto:oauth@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/oauth/. Subscribe at https://www.ietf.org/mailman/listinfo/oauth/.

Source for this draft and an issue tracker can be found at https://github.com/bc-pi/7523redux.

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 22 September 2025.

Table of Contents

1. Introduction

TODO Introduction that mentions [AUDIENCE-TAKES-SHOW] and mayby a bit of context/history and motivation for this doc that will update/patch [RFC7523], [RFC7522], and [RFC9126].

2. Conventions and Definitions

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.

3. The Updates

3.1. JWT Client Authentication

aud must solely contain the authorization server’s issuer identifier.

Explicit typing of the Client Authentication JWT as a good thing to do in general but also allowing for observerability and controle during the transition period.

3.2. SAML Client Authentication

This hasn’t been used in practice and this document will say not to ever use it going forward.

3.3. Assertion Based Authorization Grants

Advise client to ensure that the audience of the assertion makes sense with respect to where it’ s being sent, which might Token endpoint URL, Issuer Identifier, SAML Entity ID.

4. Security Considerations

This specification tightens assertion audience handling directives as a mitigation for potential attacks arising from the exploitation of ambiguities in authorization server identification allowed by [RFC7523], [RFC7522], [RFC7521], and compounded by [RFC9126].

5. IANA Considerations

5.1. OAuth URI Registry Updates

IANA is requested to update the "OAuth URI" registry [IANA.OAuth.Parameters] for the following entriest to add [[this specfication]] as an addtional refernce:

* 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

5.2. Media Type Registration

Registration is requested for the following media type in the IANA "Media Types" registry [IANA.MediaTypes] in the manner described in [RFC6838].

TODO for application/client-authentication+jwt

6. References

6.1. Normative References

[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/rfc/rfc2119>.

[RFC6749] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework", RFC 6749, DOI 10.17487/RFC6749, October 2012, <https://www.rfc-editor.org/rfc/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/rfc/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/rfc/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/rfc/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/rfc/rfc8174>.

[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/rfc/rfc9126>.

6.2. Informative References

[AUDIENCE-TAKES-SHOW]
Hosseyni, P. and T. Wrtele, "Client Assertions Gone Wrong: When the Audience Takes Over the Show", March 2024, <https://talks.secworkshop.events/osw2025/talk/R8D9BS/>.

[I-D.ietf-oauth-rfc7523bis]
Jones, M. B., Campbell, B., and C. Mortimore, "JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants", Work in Progress, Internet-Draft, draft-ietf-oauth-rfc7523bis-00, 21 February 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-oauth-rfc7523bis-00>.

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

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

[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/rfc/rfc6838>.

[RFC7515] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", RFC 7515, DOI 10.17487/RFC7515, May 2015, <https://www.rfc-editor.org/rfc/rfc7515>.

[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/rfc/rfc7519>.

[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/rfc/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/rfc/rfc8725>.

Document History

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

draft-campbell-oauth-rfc7523redux-00:

* Initial draft proposing a simipler and less distrupitve alternative to [I-D.ietf-oauth-rfc7523bis]

Acknowledgments

The authors would like to acknowledge the following people for their contributions to this document: John Bradley, Ralph Bragg, Joseph Heenan, Pedram Hosseyni, Aaron Parecki, Filip Skokan, and Tim Wrtele.

Authors' Addresses

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

Chuck Mortimore
Disney
Email: charliemortimore@gmail.com

Brian Campbell
Ping Identity
Email: bcampbell@pingidentity.com