

draft-ietf-oauth-rfc7523bis

Updates to Audience Values for OAuth 2.0 Authorization Servers

Mike Jones, Brian Campbell, Filip Skokan
IETF 123, Madrid
July 24, 2025



Fixes vulnerability exploiting ambiguous audience values for AS



- Vulnerability and specs affected described at IETF 122
- See presentation there for details
 - <https://datatracker.ietf.org/meeting/122/materials/slides-122-oauth-sessb-updating-jwt-profile-for-oauth-20-client-authentication-and-authorization-grants-00>

Updates multiple OAuth 2.0 specs



- RFC 7521 - Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants
- RFC 7522 - Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants
- RFC 7523 - JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants
- RFC 9126 - OAuth 2.0 Pushed Authorization Requests

At IETF 122, we decided to “Move fast and break fewer things”



- Targeted document focused on addressing the issue:
 - Update JWT based client authentication
 - AS Issuer Identifier as the sole audience
 - Explicit type
 - Update SAML based client authentication
 - Admit nobody does it
 - Tell people never to do it
 - Update assertion-based authorization grants
 - Advise client to ensure that the audience of the assertion makes sense with respect to where it's being sent
 - Token endpoint URL, Issuer Identifier, SAML Entity ID
- Discussed with security researchers at OSW

**PATCH rather than PUT
is RECOMMENDED**



CALYPSO'S
CONVENTION CENTER
ISLAND SPA
TOWER II & III
FITNESS CENTER
JAVA'S COFFEE CAFÉ
TOWER I

 **CARIBE ROYALE**

Developments since IETF 122



-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].

Then verified with the IESG that they are good with this approach

-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.

People have been reading it!



- Issues filed
 - <https://github.com/oauth-wg/draft-ietf-oauth-rfc7523bis/issues>
- PRs created
 - <https://github.com/oauth-wg/draft-ietf-oauth-rfc7523bis/pulls>
- Next, we'll introduce open issues for working group discussion

Issue #8 on Explicit Typing



- Should explicit typing be a MUST or a SHOULD?
- Purpose is to signal to AS that updated audience restrictions are in effect.
- Pieter, Arndt concerned MUST could be deployment blocker

Issue #9 on SAML Authorization Grants



- Requested clarifications on using SAML Authorization Grants
- “Break fewer things” changes published in -02 may have addressed this (or some of it)

Issue #12 on String “aud” Values



- “aud” with a single-valued JSON array is semantically equivalent to a JSON string
 - Spec currently mandates use of a JSON string
- Arndt Schwenkschuster pointed out that Kubernetes always uses array-valued “aud” values, even when only one audience
- Complying with mandating JSON string would require updating Kubernetes
- Should we relax to allow either a string or single-element array?

Issue #13 on Grant Audience Check



- Brian suggests shifting the responsibility of the grant audience check somewhat to the client
 - less breakage, more flexibility, same security

Issue #14: Many issues in one



- “changes after changes from one morning in Bangkok”
- Lots of detailed suggestions for us to consider
- Please see the issue

changes after changes from one morning in Bangkok #14

Open

bc-pi opened 3 days ago Member ...

Thanks for doing this [@selfissued](#)! I'm "approving" because it's a major step forward. I created issues [#12](#) and [#13](#) based on things [@arndt-s](#) noted (and personal opinion too!). Also had these notes while reviewing, which we can follow up on after "landing" this PR:

- the Abstract and intro could use some updates/clarifications based on the more targeted scope
- I think we could/should update to existing registry entries to add this doc as an additional reference so folks that might come from there will more easily find it
- not sure an update from <https://saml-sp.example.net/> to <https://authz.example.net/> in the SAML is needed.
- not sure an update to the whole SAML 2.0 Assertion example is needed
- Using JWTs for Client Authentication - the example is replaced - I'm not sure what changed to be honest and if we're gonna update/replace it, maybe we should fill it out then rather than then the [...omitted...]?
- MUST be a JSON string, and not a single-valued JSON array is noted in [aud w/ a single-valued JSON array is semantically equivalent to a JSON string #12](#)
- "client-authentication+jwt another more specific explicit type value defined by a" looks like a typo missing word, "or"
- example claims set {}'s could be rationalized
- "sub": "<mailto:mike@example.com>" in the client auth example is maybe misleading/confusing - let's revisit the details here

Originally posted by [@bc-pi](#) in [#10 \(review\)](#)

Issue #16: Improve Specification Title



- Mike Schwartz suggested
 - Updates to Audience Values Sent to OAuth 2.0 Authorization Servers
- over the current
 - Updates to Audience Values for OAuth 2.0 Authorization Servers
- Another possible title is
 - Updates to Audience Values Intended for OAuth 2.0 Authorization Servers
- Another another possible title is
 - Updates to OAuth 2.0 Client Assertion Authentication and Assertion-based Authorization Grants

Next Steps



- Continue discussing details of the changes made
 - And their implications both for security and adoption
- Update the draft to incorporate conclusions and publish
- Iterate until ready for WGLC
- Timely publication a goal
 - The Security ADs and OAuth chairs assured us that draft can be expedited in several ways, when ready
 - Let's get it ready!