IETF 124, Montreal
OAuth WG
November 2025

Michael B. Jones (Self-Issued Consulting)
Brian Campbell (Ping Identity)
Chuck Mortimore (Disney)
Filip Skokan (Okta)

draft-ietf-oauth-rfc7523bis:

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

https://datatracker.ietf.org/doc/draft-ietf-oauth-rfc7523bis/

It all started* at OSW ‘25

*

OpenID

OpenID Foundation
5000 Executive Parkway Su
San Ramon, CA 94583
United States

January 24, 2025

Dear OpenID Foundation Community,

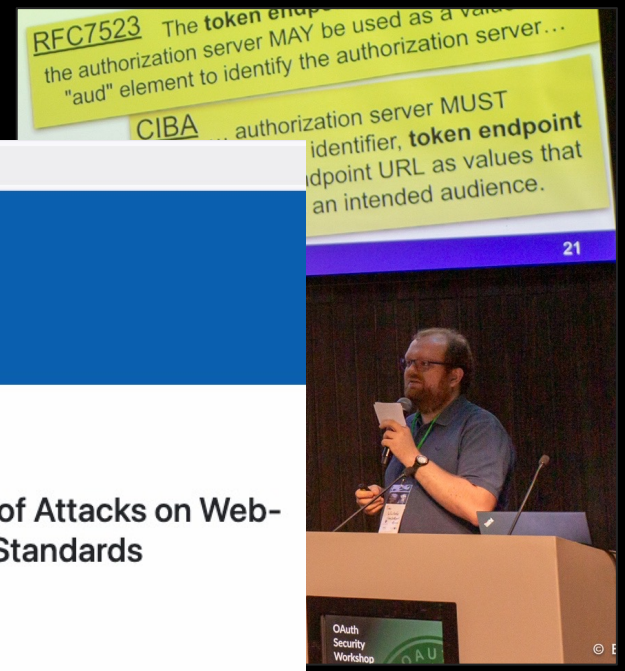
Overview

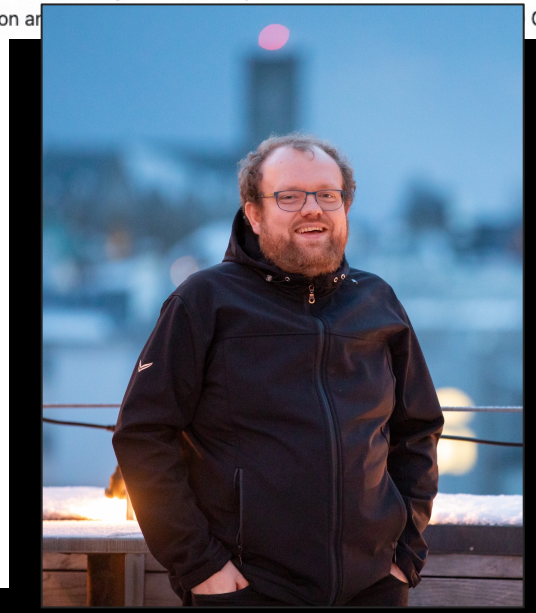
This note discloses a security vulnerability related to use of `private_key_jwt`.

We are not aware of any known compromises based on this potential attack vector. Today, we are advising all implementers that they may be impacted and sharing guidance about how to protect your implementations.

Confidentiality

To protect implementations across the supply chain, we request you consider this information as **highly sensitive:** please do not publish the letter or details of the attack while the community works on the remediation steps. This helps to ensure that an academic or theoretical risk will not be exploited by bad actors.

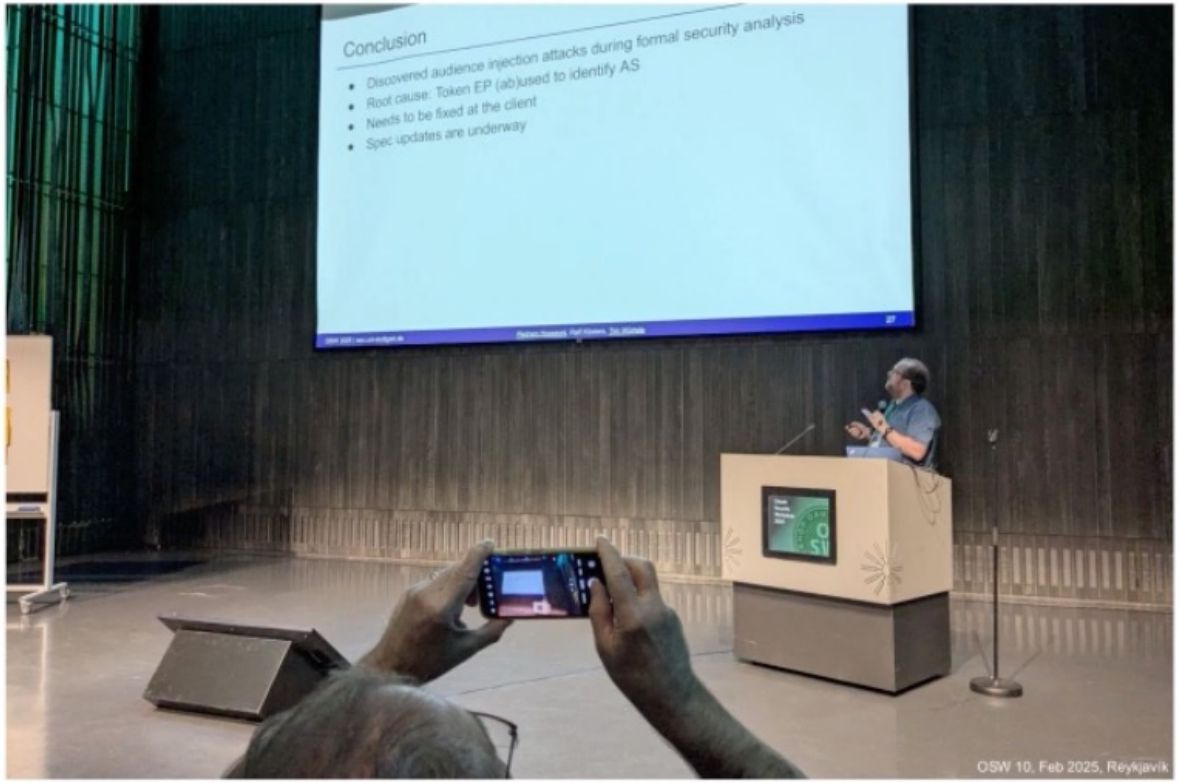




IETF122
OAUTH

So meta it hurts

Meta-analogy



22

Speaking: []

IETF 122: Web Authorization Protocol (OAUTH) 2025-03-21 02:30

IETF - Internet Engineering Task Force
10.9K subscribers

Subscribe

3 Share Ask

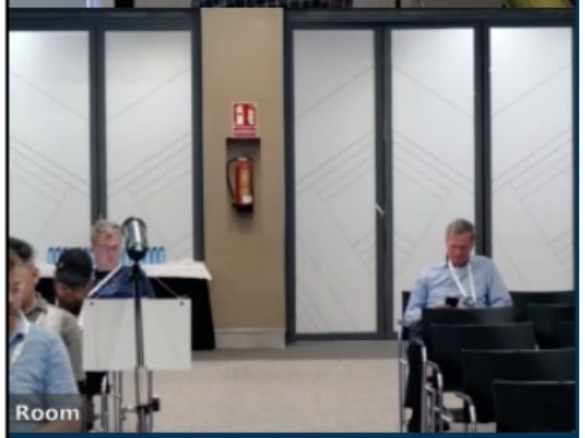
IETF123 OAUTH

122 at 123 at 124

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

4



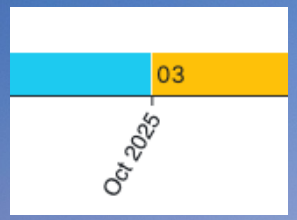
Speaking: []

IETF 123: Web Authorization Protocol (OAUTH) 2025-07-24 07:30

IETF - Internet Engineering Task Force
10.9K subscribers
Subscribe

0 Share Ask

Since IETF 123 Madrid



-03

- Update OAuth Token Endpoint Authentication Methods IANA entries with reference to this specification
- Do not restrict the "aud" claim's type. Allow it to be an array with a single member.
- Advise the client to ensure that the audience of an assertion authorization grant makes sense with respect to where it’s being sent.
- Updates to the abstract and introduction to (hopefully) better reflect the more targeted scope of the work.
- Remove JWTs for Client Authentication example replacement (not worth it for including typ in the encoded JWT header).
- Add request to update existing OAuth URI registrations to add reference to this specification for the four relevant URNs.
- Fixup the new Client Authentication JWT Example.

also in -03:

New Title!

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 o

Internet-Dra
Task Force (
working docu
Drafts is at

Internet-Dra
and may be u
time. It is
material or

This Interne

Copyright Notic

Copyright (c
document auth

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

Jones, et al. Expires 23 January 2026 [Page 1]
Internet-Draft Updates to Audience Values for ASs July 2025

draft-ietf-oauth-rfc7523bis.xml Outdated Hide resolved

```
19  19
20  20      <front>
21      -     <title abbrev="Updates to Audience Values for ASs">Updates to Audience Values for OAuth 2.
        21  +     <title>Updates to OAuth 2.0 JSON Web Token (JWT) Client Authentication and Assertion-Based
```

bc-pi 27 days ago • edited Member

By accident while looking at some other draft I noticed that the abbrev value does show up in the footer of the txt version rendered under the other stuff on the main datatracker page https://datatracker.ietf.org/doc/draft-ietf-oauth-rfc7523bis/ so there we should probably consider adding something short and without the word "ass".

Updates to OAuth 2.0 JSON Web Token (JWT) Client Authentication and Assertion-Based Authorization Grants
draft-ietf-oauth-rfc7523bis-03

Abstract

This specification updates the requirements for 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.

ıce with the

ːnet Engineering
ːo distribute
ˈ current Internet-
ːurrent/.

ːximum of six months
ːr documents at any
as reference
ːogress."

ˈ.

Copyright Notice

Copyright (c) 2025 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.

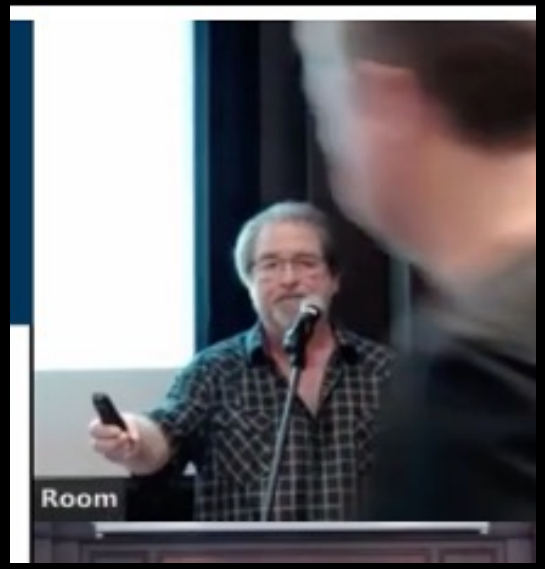
Jones, et al. Expires 23 January 2026 [Page 1]
Internet-Draft JWT Client Auth Updates July 2025


FIN
?
I think that's French for is it time to consider WGLC?

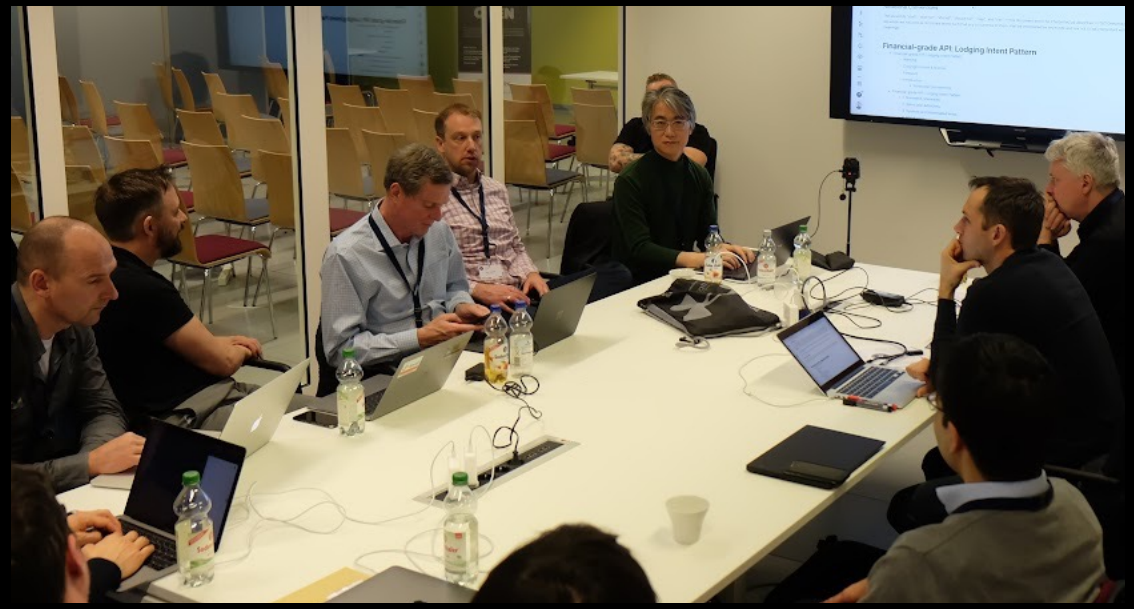
Postscript:
Too meta for my shirt

IETF 123
July 2025
Madrid

OSW 7
May 2022
Trondheim



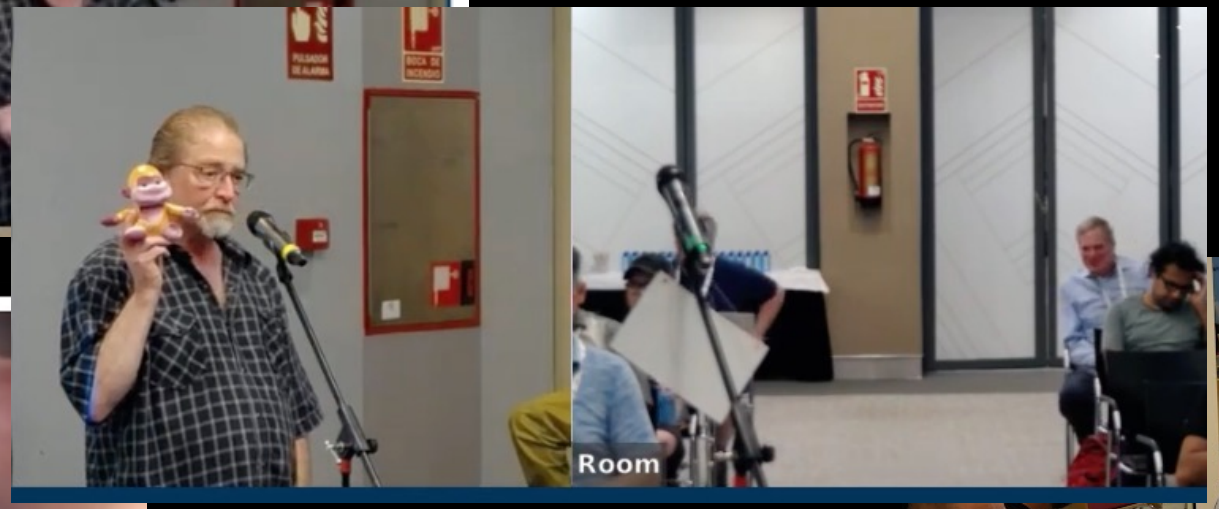
IETF 122
March 2025
Bangkok

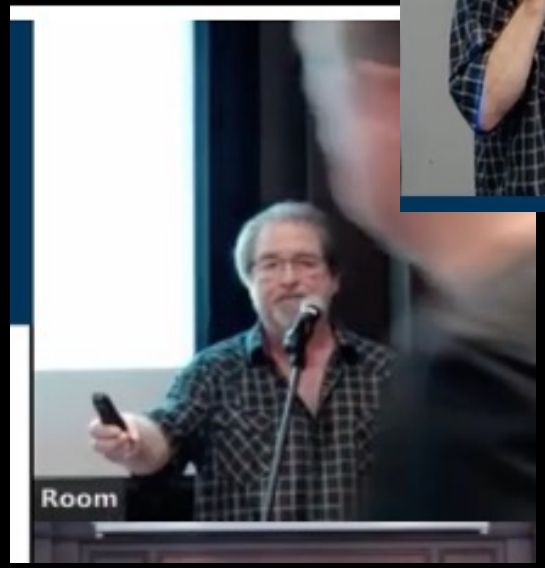


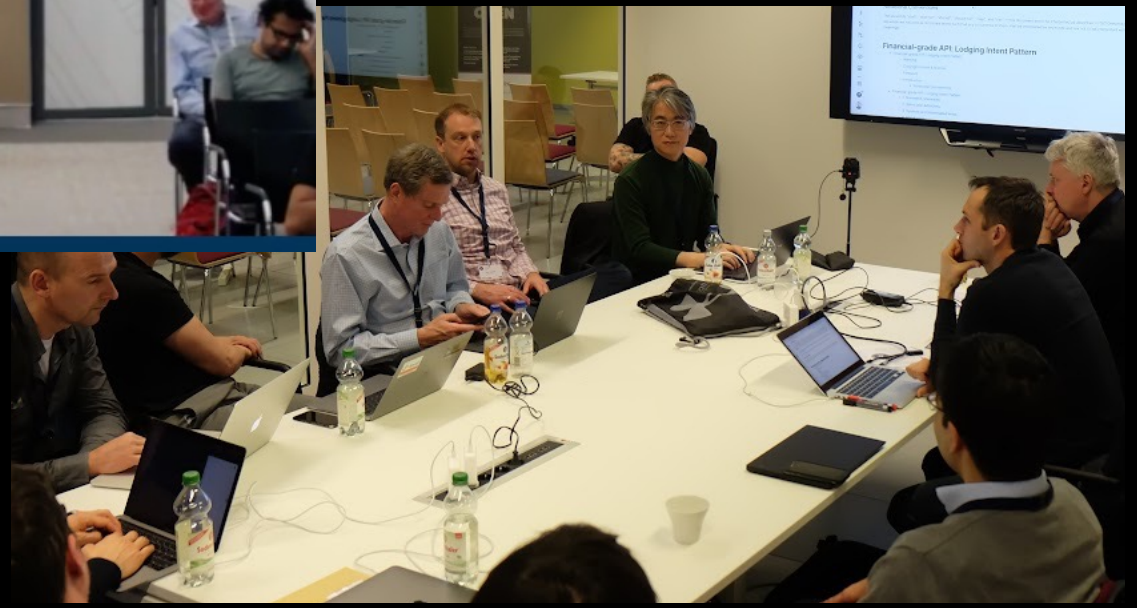
OSW 4
March 2019
Stuttgart

Postscript:
Too meta for my shirt

IETF 123
July 2025
Madrid







OSW 4
March 2019
Stuttgart