Progress Report on Handling an Actionable Security Vulnerability

May 27, 2026

Michael B. Jones

Self-Issued Consulting

Security Analysis of Our Specifications

- Formal analysis of OAuth 2 led to the first OAuth Security Workshop – Darmstadt, November 2015
  - Analysis by Guido Schmitz and Daniel Fett under the supervision of Professor Ralf Küsters
  - Identified the “mix-up” attack
- OpenID Foundation commissions security analysis of key specs
  - FAPI 1, FAPI 2, FAPI-CIBA, OpenID4VC, OpenID Federation, etc.
- Security researchers at University of Stuttgart perform formal analysis of specifications for the OpenID Foundation

2024 Security Analysis of OpenID Federation

- Stuttgart security researchers analyzed Last OpenID Federation Implementer's Draft in mid-2024
  - Tim Würtele, Pedram Hosseyni, and Professor Ralf Küsters
- Discovered an actionable security vulnerability in the audience values used for JWT Client Authentication and/or PAR
  - Applies to numerous specs using JWT Client Authentication and/or PAR, including multiple OAuth specifications
- Privately reported to the OIDF on September 20, 2024

Rest of This Presentation to Cover

- What happened next and why?
- How the vulnerability was:
  - Discussed privately among authors of affected specifications
  - Disclosed to affected parties and developers
  - Disclosed to the OAuth working group
  - Disclosed publicly by the OpenID Foundation
  - Fixed in the affected specifications (still a work in progress)
- Tradeoffs considered and decisions made
- Lessons learned

- *Much of this information not previously public*

Pre-Disclosure Timeline: September 2024

- Sep 20: Researchers e-mailed me about the vulnerability
  - Described how malicious authorization server could use the token endpoint of a legitimate authorization server as the audience value
  - Resulting in a client authentication JWT the attacker can use there
  - Initial description was of how PAR is vulnerable
- Sep 20: I looped in other OpenID Federation authors
- Sep 23: Pedram Hosseyni wrote
  - “We agree that the best fix is to mandate either the issuer identifier (done, e.g., in FAPI 2.0) or the exact endpoint at which the is used (e.g., the PAR endpoint for PAR requests, and the token endpoint for token requests) as the audience value.”
- Sep 23: Giuseppe De Marco advocated for responsible disclosure, given the broad impact of the vulnerability

Pre-Disclosure Timeline: Sep-Oct 2024

- Sep 25: Tim Würtele clarified that the fix requires changes to the audience values used by clients
  - He advocated for using the issuer identifier value as “aud” like FAPI 2.0 does
- Oct 2: Tim and Pedram supplied write-up on the attack as it applies to OpenID Connect and PAR
- Oct 2: I shared the vulnerability with authors of PAR, OpenID Connect, OpenID Federation, and FAPI
- Oct 3: Joseph Heenan shared with key OIDF staff and identified potentially affected Open Finance and Open Insurance ecosystems
- Oct 4: Pedram pointed out that CIBA is also vulnerable
- Oct 9: Filip Skokan suggested updating RFC 7523 and OpenID Connect and pointed out the need to update certification tests allowing audience arrays

Pre-Disclosure Timeline: Oct-Dec 2024

- Oct 10: Planning call among OpenID and OAuth editors
- Oct 24: OpenID Federation draft 40 published with change to use the issuer identifier as the audience *(without saying why)*
- Nov 5: Invitation-only discussion at IETF 121 in Dublin
  - Discussed pros and cons of potential solutions
  - Filip Skokan proposed explicitly typing `private_key_jwt` JWTs in rfc7523bis
- Nov 27: Non-publicized draft-jones-oauth-rfc7523bis GitHub draft created
- Dec 2: FAPI 2 updated to require issuer identifier as only “aud” value *(without saying why)*
- Nov & Dec: “Responsible Disclosure” doc privately shared with potentially vulnerable FAPI ecosystems and vendors
- December: Fixes applied to SDKs, such as Connect2ID, Duende

Pros and Cons of Proposed Solutions *(from IETF 121 Private Meeting)*

	“aud” = Issuer Identifier	**“aud” = Target Endpoint**	**New claim like “htu”**
Pros	Aligns w/ RFC 9207 “iss” Aligns w/ RFC 8414 issuer Single identifier for each AS Used in FAPI 2 security analysis Used in OpenID Federation	Usable in systems w/o issuer identifier (but not having it seems unlikely when client uses multiple ASs) Aligns w/ part of RFC 7523 token endpoint URL guidance	New claim that we can define however we like Doesn’t require updating description of “aud” anywhere
Cons	Requires spec updates Requires updates to some software using private_key_jwt Alternative needed when no issuer in ecosystem (like RFC 9207 “deployment-specific ways” alternative)	Requires spec updates Requires updates to some software using private_key_jwt Many identifiers for same AS (one per endpoint) – confusing *May not solve the security problem* when endpoints shared by multiple ASs	Requires spec updates Requires updates to **all** software using private_key_jwt Gives up on purpose of “aud” Duplicates purpose of “aud”

Partial-Disclosure Timeline: January 2025

- Jan 24: Vulnerability described in non-publicized OpenID page
  - https://openid.net/wp-content/uploads/2025/01/OIDF-Responsible-Disclosure-Notice-on-Security-Vulnerability-for-private_key_jwt.pdf
- Jan 27: draft-jones-oauth-rfc7523bis published
- Jan 27: OAuth special topic call on security vulnerability
  - Presentation by Joseph Heenan and Mike Jones
- Jan 31: Security analysis of OpenID Federation ID4 delivered

Key Slides from Jan 25, 2025 OAuth Virtual Interim

Special Topic Call on the Security Vulnerability

Requirements to perform attack / mitigations

- Attack should not be possible if MTLS is used and MTLS certificate is required to match client id
- Requires attacker to have registered a bank or gained control of a bank
- Probably requires 2+ endpoints with client authentication (e.g. PAR + token endpoint)
- client_id needs to be same across both AS (attacker can control if DCR used)
- FAPI2ID2 requires that client send aud == issuer
- Some ecosystems plan to ask AS to reject if aud != issuer

Pros and Cons of Possible Solutions

	“aud” = Issuer Identifier	“aud” = Target Endpoint	New claim like “htu”
Pros	Aligns w/ RFC 9207 “iss” Aligns w/ RFC 8414 issuer Single identifier for each AS Used in FAPI 2 security analysis Used in OpenID Federation	Usable in systems w/o issuer identifier (but not having it seems unlikely when client uses multiple ASs) Aligns w/ part of RFC 7523 token endpoint URL guidance	New claim that we can define however we like Doesn’t require updating description of “aud” anywhere
Cons	Requires spec updates Requires updates to some software using private_key_jwt Alternative needed when no issuer in ecosystem (like RFC 9207 “deployment-specific ways” alternative)	Requires spec updates Requires updates to some software using private_key_jwt Many identifiers for same AS (one per endpoint) – confusing *May not solve the security problem* when endpoints shared by multiple ASs	Requires spec updates Requires updates to **all** software using private_key_jwt Gives up on purpose of “aud” Duplicates purpose of “aud”

Solution that Gained Consensus

“aud”=Issuer Identifier
- Issuer Identifier introduced by AS Metadata spec [RFC 8414]
- Single unambiguous identifier for the AS

Already used by most modern specs as AS “aud” value
- Recommended by PAR [RFC 9126]
- Used by JAR [RFC 9101]
- Used by OpenID FAPI 2
- Used by OpenID Federation
- Used by OAuth “iss” Parameter [RFC 9207]

Also enable explicit typing (“typ”=”...+jwt”) in updated specs
- Enables participants to know that updated specs being used

Solution Applied: Proposed Spec Updates

- OAuth JWT Assertions [RFC 7523]
- OAuth Assertion Framework [RFC 7521]
- OAuth SAML Assertions [RFC 7522]
- OpenID Connect Core
- OpenID FAPI 1
- OpenID FAPI 2
- OpenID Federation
- OpenID Client-Initiated Backchannel Authentication (CIBA)
- OAuth JWT Authorization Request (JAR) [RFC 9101]
- OAuth Pushed Authorization Request (PAR) [RFC 9126]
- OAuth Security BCP [RFC-to-be 9700]

Outcomes from Jan 27, 2025 OAuth Interim

OAuth special topic call on security vulnerability

- Decided to update JWT Assertions [RFC 7523], PAR [RFC 9126]
- Decided not to delay publication of OAuth Security BCP *(now RFC 9700)* to describe vulnerability and apply fix
- Decided to start adoption call for draft-jones-oauth-rfc7523bis

Partial-Disclosure Timeline: February 2025

- Feb 10: Talk by Tim and Pedram at OSW Iceland
  - Emphasized that fix must occur in the client
- Feb 21: draft-ietf-oauth-rfc7523bis-00 published after successful call for adoption of draft-jones-oauth-rfc7523bis

Post-Disclosure Timeline: Feb-Mar 2025

- Feb 25: Public blog post disclosing vulnerability
  - https://openid.net/notice-of-a-security-vulnerability/
- Mar 21: Mike Jones and Brian Campbell discuss rfc7523bis during OAuth meeting at IETF 122 in Bangkok
  - Discussed tradeoffs on scope of changes to apply to OAuth specs
  - WG decision to “Move fast and break fewer things”
    - Update JWT-based client authentication in RFC 7523
    - Make non-breaking updates to assertion-based authorization grants
    - Deprecate SAML-based client authentication
  - Decision to make all updates in rfc7523bis and not replace RFC 7523

rfc7523bis Work Applying IETF 122 Decisions

- Apr 23, 2025: rfc7523bis-01 published
  - Revisions to update rather than replace RFC 7523
  - Removed updates to JAR [RFC 9101], since desired audience behavior was already a SHOULD there
  - Referenced Stuttgart Audience Injection Attacks paper
- Jul 22, 2025: rfc7523bis-02 published
  - Applied “Move fast, break fewer things” decisions from IETF 122
    - Focused RFC 7523 updates on JWT client authentication case
    - Removed new “aud” requirements for JWT authorization grants
    - Deprecated use of SAML assertions for client authentication
  - Added Filip Skokan as an author

Applying More rfc7523bis Input from the WG

- Jul 21-25, 2025: Discussions at IETF 123 in Madrid
  - Lots of feedback about deployment and compatibility considerations
- Oct 7, 2025: rfc7523bis-03 published
  - Make use of strongly typed JWTs a SHOULD rather than a MUST
  - Let “aud” be a single-valued array rather than requiring a string value

  - *Both changes motivated by Kubernetes deployment considerations*

IETF Process Playing Out for rfc7523bis

- Nov 17, 2025: Working Group Last Call started
- Jan 9, 2026: Published rfc7523bis-04 applying WGLC feedback
- Jan 26, 2026: Published rfc7523bis-05 applying suggestions by Axel Nennker
- Mar 11, 2026: Published rfc7523bis-06 applying shepherd feedback
- Apr 10, 2026: Published rfc7523bis-07 addressing AD feedback
- Apr 16-May 20, 2026: Published -08 to -11 addressing directorate and IESG feedback
- May 4, 2026: Specification sent to RFC Editor
- May 6, 2026: IANA registrations performed

Second OpenID Federation Security Analysis

- Security analysis of Final OpenID Federation 1.0 specification began April 2026
  - University of Stuttgart security researchers conducting this analysis
  - Updates the formal model used in analysis to match the final spec
  - Will verify that audience security vulnerability fixed
  - Will verify that Federation Identity and Metadata Integrity achievable
- Preliminary report describing the model being used for analysis e-mailed to the working group on May 11, 2026

Reflection

- What we did well on
  - We quickly agreed on a simple, common fix for all affected specs
  - We quickly responsibly disclosed vulnerability to affected parties
  - Implementations and deployments were updated before disclosure
- What we could have done better on
  - We intended to update the specs fast but it's taken 20 months
    - Progress eventually fell into the normal cadence of IETF spec development
  - Updated versions of OpenID Connect, OAuth Security BCP, etc. waiting on rfc7523bis RFC

Your Turn!

- What would you like to add to our collective reflection on this journey?

- *Slides will be posted at https://self-issued.info/*