Web Authorization Protocol
Internet-Draft
Intended status: Informational
Expires: 29 December 2025

J. Richer
Bespoke Engineering
B. Campbell
Ping Identity
D. H. Saxe
Full Frontal Nerdity Industries

27 June 2025

Deferred Key Binding for OAuth
draft-richer-oauth-tmb-claim-01

Abstract

Sometimes you want to get a token that’s tied to a public key but you can’t prove possession of that public key. That’s when you need to trust me, bruh.

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://jricher.github.io/draft-richer-oauth-tmb-claim/draft-richer-oauth-tmb-claim.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-richer-oauth-tmb-claim/.

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/jricher/draft-richer-oauth-tmb-claim.

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/.

Copyright Notice

Table of Contents

1. Introduction

The JWT confirmation claim "cnf" [RFC7800] allows an RS to determine PoP semantics for a token. However, methods like mTLS [RFC8705] and DPoP [RFC9449] assume that the requester of that token can prove possession of the key that is bound to the token. Sometimes that's just too hard, and so here we define a claim to allow a requester to ask for a token that is bound to a key that the requester cannot, does not want to, or does not feel like proving possession of at the time of request.

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. Token Meta-key Binding Claim

The token meta-key binding "tmb" claim is passed in an OAuth token request parameter of the same name. Its value is the form-encoded value that the requester wants the confirmation claim to be in the issued token. If the requester is making a DPoP or mTLS request, any keys there MUST be ignored.

The same parameter can be used in a token exchange request, with the same results.

If the issued token is a JWT, the value of the "tmb" claim is copied to the "cnf" claim of the resulting token. If the token is introspected, the value of "tmb" is returned in the "cnf" claim of the introspection response.

The requester SHOULD give the resulting token to the holder of the key represented in the "tmb" claim.

The presenter of the token MUST prove possession of the key in the resulting "cnf" claim using the appropriate key validation method for the type of token.

4. Security Considerations

The security of this specification is entirely based on trust. If you have trust issues, it’s not going to be secure.

5. IANA Considerations

This document registers the "tmb" claim to the IANA JWT Claims registry and OAuth request parameter.

6. 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>.

[RFC7800] Jones, M., Bradley, J., and H. Tschofenig, "Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)", RFC 7800, DOI 10.17487/RFC7800, April 2016, <https://www.rfc-editor.org/rfc/rfc7800>.

[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>.

[RFC8705] Campbell, B., Bradley, J., Sakimura, N., and T. Lodderstedt, "OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens", RFC 8705, DOI 10.17487/RFC8705, February 2020, <https://www.rfc-editor.org/rfc/rfc8705>.

[RFC9449] Fett, D., Campbell, B., Bradley, J., Lodderstedt, T., Jones, M., and D. Waite, "OAuth 2.0 Demonstrating Proof of Possession (DPoP)", RFC 9449, DOI 10.17487/RFC9449, September 2023, <https://www.rfc-editor.org/rfc/rfc9449>.

Acknowledgments

TODO acknowledge.

Authors' Addresses

Justin Richer
Bespoke Engineering
Email: ietf@justin.richer.org

Brian Campbell
Ping Identity
Email: bcampbell@pingidentity.com

Dean H. Saxe
Full Frontal Nerdity Industries
Email: dean@thesax.es