OAuth Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 10, 2020

M. Jones
Microsoft
B. Campbell, Ed.
Ping Identity
J. Bradley
Yubico

March 9, 2020

OAuth 2.0 DPoP for the Implicit Flow
draft-jones-oauth-dpop-implicit-00

Abstract

This specification describes a mechanism for sender-constraining OAuth 2.0 tokens via a proof-of-possession mechanism on the application level. This mechanism allows for the detection of replay attacks with access tokens.

This specification compliments and builds upon the mechanisms defined in draft-fett-oauth-dpop, in which access tokens are returned from the token endpoint. In particular, this specification extends the Demonstration of Proof-of-Possession at the Application Layer (DPoP) mechanisms to also be usable with the OAuth 2.0 implicit flow, in which access tokens are returned from the authorization endpoint.

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 September 10, 2020.

Table of Contents

1. Introduction

This specification defines additions to the mechanisms defined in [I-D.fett-oauth-dpop] enabling Demonstration of Proof-of-Possession at the Application Layer (DPoP) mechanisms to be used with the OAuth 2.0 implicit flow, in which access tokens are returned from the authorization endpoint. These additions are intended for use with these "response_type" values: "token", "id_token token", "code token", and "code id_token token".

1.1. Requirements Notation and Conventions

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.

1.2. Terminology

This specification uses the terms "access token", "authorization endpoint", "authorization request", and "token endpoint" defined by The OAuth 2.0 Authorization Framework [RFC6749].

2. DPoP for the Implicit Flow

Demonstration of Proof-of-Possession at the Application Layer (DPoP) for the implicit flow is performed in the same manner as [I-D.fett-oauth-dpop], with this exception: Rather than sending the DPoP proof JWT in a DPoP HTTP header, the DPoP proof JWT is instead sent as the value the new "dpop" OAuth request parameter, which is defined in this section.

2.1. DPoP OAuth Request Parameter

This specification defines the following OAuth request parameter for use at the authorization endpoint:

dpop
: The DPoP proof JWT for requests using the implicit flow.

2.2. DPoP Proof JWT for the Implicit Flow

DPoP proof JWTs used with the implicit flow are as specified in [I-D.fett-oauth-dpop], with the following modifications.

- The value of the "htm" claim MUST be the HTTP verb used in the authorization request, which is normally "GET".
- The value of the "htu" claim MUST be the URL of the authorization endpoint used in the request.

3. Security Considerations

The security considerations described in [I-D.fett-oauth-dpop] also apply to this specification.

4. IANA Considerations

4.1. OAuth Parameters Registration

This specification registers the following value in the IANA "OAuth Parameters" registry [IANA.OAuth.Parameters] established by [RFC6749].

4.1.1. Registry Contents

- Parameter name: dpop
- Parameter usage location: authorization request
- Change controller: IESG
- Specification document(s): Section 2.1 of [[this specification]]

5. References

5.1. Normative References

[I-D.fett-oauth-dpop]
Fett, D., Campbell, B., Bradley, J., Lodderstedt, T., Jones, M., and D. Waite, "OAuth 2.0 Demonstration of Proof-of-Possession at the Application Layer (DPoP)", draft-fett-oauth-dpop-04 (work in progress), March 2020.

[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/info/rfc2119>.

[RFC6749] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework", RFC 6749, DOI 10.17487/RFC6749, October 2012, <https://www.rfc-editor.org/info/rfc6749>.

[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/info/rfc8174>.

5.2. Informative References

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

Appendix A. Document History

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

-00

o Initial version.

Authors' Addresses

Michael B. Jones
Microsoft

Email: mbj@microsoft.com
URI: https://self-issued.info/

Brian Campbell (editor)
Ping Identity

Email: brian.d.campbell@gmail.com

John Bradley
Yubico

Email: ve7jtb@ve7jtb.com