

Web Authorization Protocol  
Internet-Draft  
Intended status: Standards Track  
Expires: 21 April 2026

A. Parecki  
Okta  
18 October 2025

OAuth 2.0 JWT Authorization Grant with DPoP Binding  
draft-parecki-oauth-jwt-dpop-grant-00

## Abstract

This specification defines a new OAuth 2.0 authorization grant type that uses a JSON Web Token (JWT) assertion to request an access token that is bound to a specific key using the Demonstration of Proof-of-Possession (DPoP) mechanism. This provides a higher level of security than a simple bearer token, as the client must prove possession of the key to use the access token.

## 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://drafts.aaronpk.com/oauth-jwt-dpop-grant/draft-parecki-oauth-jwt-dpop-grant.html>. Status information for this document may be found at <https://datatracker.ietf.org/doc/draft-parecki-oauth-jwt-dpop-grant/>.

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/aaronpk/oauth-jwt-dpop-grant>.

## 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 21 April 2026.

## 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. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. Conventions and Definitions . . . . .	3
2.1. Terminology . . . . .	3
3. HTTP Parameter Bindings for Transporting Assertions . . . . .	3
3.1. Using DPoP-Bound JWTs as Authorization Grants . . . . .	3
4. JWT Format and Processing Requirements . . . . .	4
4.1. Access Token Response . . . . .	5
5. Security Considerations . . . . .	5
6. IANA Considerations . . . . .	5
6.1. OAuth URI Registration . . . . .	5
7. Normative References . . . . .	5
Acknowledgments . . . . .	6
Author's Address . . . . .	6

## 1. Introduction

The JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants [RFC7523] defines the use of a JWT as an authorization grant, using the grant type `urn:ietf:params:oauth:grant-type:jwt-bearer`. This grant type describes the use of a JWT authorization grant as a bearer token, which is susceptible to reuse by any party that obtains one.

OAuth 2.0 Demonstration of Proof-of-Possession at the Application Layer (DPoP) [RFC9449] defines a mechanism to bind access tokens to a specific cryptographic key. This prevents the token from being used by any party that does not have access to the private key.

This specification extends the proof-of-possession concept to the authorization grant itself. It defines a new grant type, `urn:ietf:params:oauth:grant-type:jwt-dpop`, for cases where the JWT assertion is already bound to a DPoP key. To exchange the assertion for an access token, the client must provide a DPoP proof demonstrating possession of the key to which the assertion is bound. This makes the JWT assertion a sender-constrained credential.

## 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.

### 2.1. Terminology

This specification uses the terminology of [RFC6749], [RFC7521], [RFC7523], and [RFC9449].

## 3. HTTP Parameter Bindings for Transporting Assertions

The OAuth Assertion Framework [RFC7521] defines generic HTTP parameters for transporting assertions (a.k.a. security tokens) during interactions with a token endpoint. This section defines specific parameters and treatments of those parameters for use with JWT DPoP-Bound Tokens.

### 3.1. Using DPoP-Bound JWTs as Authorization Grants

To use a DPoP-bound JWT as an authorization grant, the client uses an access token request as defined in Section 4 of [RFC7521] with the following specific parameter values and encodings.

`grant_type`: REQUIRED - The value MUST be `urn:ietf:params:oauth:grant-type:jwt-dpop`

`assertion`: REQUIRED - A single JWT, as defined in [RFC7519], that contains a `cnf` claim as described in Section 4.

`scope`: OPTIONAL - The scope parameter may be used, as defined in [RFC7521], to indicate the requested scope.

Authentication of the client is optional, as described in Section 3.2.1 of [RFC6749] and consequently, the `client_id` is only needed when a form of client authentication that relies on the parameter is used.

The client MUST also include a DPoP header as defined in Section 4 of [RFC9449], which constitutes a proof of possession for the key to which the assertion is bound.

The following example demonstrates an access token request with a JWT as an authorization grant (with extra line breaks for display purposes only):

```
POST /token HTTP/1.1
Host: as.example.com
Content-Type: application/x-www-form-urlencoded
DPoP: eyJ0eXAiOiJkcG9wK2p3dCI6ImFsZyI6IkVTMjU2IiwiaWandrI...

grant_type=urn%3Aietf%3Aparams%3Aoauth%3Agrant-type%3Ajwt-dpop
&assertion=eyJhbGciOiJFUzI1NiIsImtpZCI6IjE2In0.
eyJpc3Mi[...omitted for brevity...].
J9l-ZhwP[...omitted for brevity...]
```

#### 4. JWT Format and Processing Requirements

The authorization server MUST validate the JWT according to the criteria below. Application of additional restrictions and policy are at the discretion of the authorization server.

1. The authorization server MUST validate the DPoP proof in the DPoP header as described in Section 4 of [RFC9449]. The `htm` claim of the DPoP JWT MUST be `POST`, and the `htu` claim must match the token endpoint URL.
2. The authorization server MUST validate the JWT assertion according to the processing rules in Section 3.1 of [RFC7523] and Section 4 of [I-D.ietf-oauth-rfc7523bis].
3. The authorization server MUST verify that the JWT assertion contains a `cnf` claim as defined in [RFC7800]. This `cnf` claim MUST contain a `jwk` property representing a public key.
4. The authorization server MUST verify that the public key in the `jwk` property of the `cnf` claim of the JWT assertion exactly matches the public key in the `jwk` header of the DPoP proof.

If any of these validation steps fail, the authorization server MUST return an `invalid_grant` error response.

#### 4.1. Access Token Response

If the request is valid, the authorization server issues an access token. The issued access token SHOULD also be DPoP-bound to the same key from the DPoP proof. In this case, the `token_type` of the access token MUST be DPoP, and the response MUST include a `token_type` parameter with the value DPoP. If a bearer token is issued, the `token_type` MUST be Bearer.

#### 5. Security Considerations

The security considerations described within the following specifications are all applicable to this document: "Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants" [RFC7521], "JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants" [RFC7523], "Updates to OAuth 2.0 JSON Web Token (JWT) Client Authentication and Assertion-Based Authorization Grants" [I-D.ietf-oauth-rfc7523bis], "OAuth 2.0 Demonstrating Proof of Possession (DPoP)" [RFC9449], "The OAuth 2.0 Authorization Framework" [RFC6749], and "JSON Web Token (JWT)" [RFC7519].

#### 6. IANA Considerations

##### 6.1. OAuth URI Registration

This specification requests registration of the following value in the "OAuth URI" registry established by [RFC6755].

- \* URN: urn:ietf:params:oauth:grant-type:jwt-dpop
- \* Common Name: DPoP-bound JWT Authorization Grant
- \* Change Controller: IESG
- \* Specification Document(s): this document

#### 7. Normative References

[I-D.ietf-oauth-rfc7523bis]

Jones, M. B., Campbell, B., Mortimore, C., and F. Skokan, "Updates to OAuth 2.0 JSON Web Token (JWT) Client Authentication and Assertion-Based Authorization Grants", Work in Progress, Internet-Draft, draft-ietf-oauth-rfc7523bis-03, 7 October 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-oauth-rfc7523bis-03>>.

- [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>>.
- [RFC6749] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework", RFC 6749, DOI 10.17487/RFC6749, October 2012, <<https://www.rfc-editor.org/rfc/rfc6749>>.
- [RFC6755] Campbell, B. and H. Tschofenig, "An IETF URN Sub-Namespace for OAuth", RFC 6755, DOI 10.17487/RFC6755, October 2012, <<https://www.rfc-editor.org/rfc/rfc6755>>.
- [RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <<https://www.rfc-editor.org/rfc/rfc7519>>.
- [RFC7521] Campbell, B., Mortimore, C., Jones, M., and Y. Goland, "Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants", RFC 7521, DOI 10.17487/RFC7521, May 2015, <<https://www.rfc-editor.org/rfc/rfc7521>>.
- [RFC7523] Jones, M., Campbell, B., and C. Mortimore, "JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants", RFC 7523, DOI 10.17487/RFC7523, May 2015, <<https://www.rfc-editor.org/rfc/rfc7523>>.
- [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>>.
- [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.

#### Author's Address

Aaron Parecki  
Okta  
Email: [aaron@parecki.com](mailto:aaron@parecki.com)