OAuth Working Group	B. Campbell
Internet-Draft	G. Liu
Intended status: Standards Track	Ping Identity
Expires: August 27, 2015	February 23, 2015

Destination Claim for JSON Web Token

draft-campbell-oauth-dst4jwt-00

Abstract

The Destination Claim for JSON Web Token (JWT) provides a means of indicating the address to which the JWT is sent. The Claim can be used to preventing malicious forwarding or redirection of a JWT to unintended recipients.

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 http://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 August 27, 2015.

Copyright Notice

Copyright (c) 2015 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 (http://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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

JWT [I-D.ietf-oauth-json-web-token] is a compact, URL-safe means of representing claims to be transferred between two parties. Oftentimes an HTTP 302 redirect or an auto-submitted HTML form, using the user agent as a intermediary, is employed as the method of transfer. The Destination Claim provides a standard way for for the Issuer to indicate the address to which it instructed the user agent to deliver the JWT. The recipient of the JWT can detect and prevent malicious forwarding or redirection to unintended recipients by verifying that the address conveyed by the Destination Claim matches the actual location at which the JWT was received.

While the Destination Claim bears some seeming similarity to the Audience Claim already defined in JWT, the distinction is that the Audience identifies *who* the JWT is intended for while the Destination identifies *where* the JWT is sent.

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 RFC 2119 [RFC2119].

1.2. Terminology

This specification uses the terms JSON Web Token (JWT), Issuer Claim, Claim Name, and Claim Value as defined in [I-D.ietf-oauth-json-web-token], and the term "user agent" as defined by RFC 7230 [RFC7230].

2. The Destination Claim

The Claim Name of the Destination Claim is dst and its Claim Value is a URI [RFC3986] indicating the address to which the JWT is sent. Use of this Claim is OPTIONAL but, if the Claim is present, the recipient MUST check that the URI identifies the location at which the JWT was received. If the JWT is received at a different location than the one conveyed by the value of the dst claim, then the JWT MUST be rejected.

3. IANA Considerations

3.1. JSON Web Token Claim Registration

This specification registers the Destination Claim defined herein in the IANA JSON Web Token Claims

registry defined in [I-D.ietf-oauth-json-web-token].

3.1.1. Registry Request Contents

- Claim Name: dst
- Claim Description: Destination
- Change Controller: IESG
- Specification Document(s): Section 2 of this document

4. Security Considerations

The Destination Claim defined in Section 2 provides a means to assist in detecting and preventing malicious forwarding or redirection of a JWT to unintended recipients. If, for example, an Issuer can be tricked into sending a JWT to a malicious site (perhaps due to inadequate checking of the target URI combined with Cross-Site Request Forgery) the JWT would be unusable at the legitimate site because the dst would contain a URI of the malicious site.

5. References

5.1. Normative References

[I-D.ietf-oauth-json-web-token] Jones, M., Bradley, J. and N. Sakimura, "JSON Web Token (JWT)", Internet-Draft draft-ietf-oauth-json-web-token-32, December 2014.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3986] Berners-Lee, T., Fielding, R. and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

5.2. Informative References

[RFC7230] Fielding, R. and J. Reschke, "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", RFC 7230, June 2014.

Appendix A. Open Issues

- Is there compelling reason to allow the dst Claim to accommodate multiple values? A single value is sufficient for the cases envisioned and is certainly simpler.

Appendix B. Document History

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

-00

- Gotta start somewhere...

Authors' Addresses

Brian Campbell
Ping Identity
EMail: brian.d.campbell@gmail.com

Guoping Liu
Ping Identity

EMail: gliu@pingidentity.com