Network Working Group
Internet-Draft
Intended status: Informational
Expires: July 29, 2016

T. Hardjono, Ed.
MIT
E. Maler
ForgeRock
M. Machulak
Cloud Identity
D. Catalano
Oracle

January 26, 2016

OAuth 2.0 Resource Set Registration
draft-hardjono-oauth-resource-reg-07

Abstract

This specification defines a resource set registration mechanism between an OAuth 2.0 authorization server and resource server. The resource server registers information about the semantics and discovery properties of its resources with the authorization server.

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 July 29, 2016.

Table of Contents

1. Introduction

There are various circumstances under which an OAuth 2.0 [OAuth2] resource server may need to communicate information about its protected resources to its authorization server:

- In some OAuth 2.0 deployments, the resource server and authorization server are operated by the same organization and deployed in the same domain, but many resource servers share a single authorization server (a security token service (STS) component). Thus, even though the trust between these two is typically tightly bound, there is value in defining a singular standardized resource protection communications interface between the authorization server and each of the resource servers.

- In some deployments of OpenID Connect [OpenIDConnect], which has a dependency on OAuth 2.0, the OpenID Provider (OP) component is a specialized version of an OAuth authorization server that brokers availability of user attributes by dealing with an ecosystem of attribute providers (APs). These APs effectively function as third-party resource servers. Thus, there is value in defining a mechanism by which all of the third-party APs can communicate with a central OP, as well as ensuring that trust between the authorization server and resource servers is able to be established in a dynamic, loosely coupled fashion.

- In some deployments of User-Managed Access [UMAcore], which has a dependency on OAuth 2.0, an end-user resource owner (the "user" in UMA) may choose their own authorization server as an independent cloud-based service, along with using any number of resource servers that make up their "personal cloud". Thus, there is value in defining a mechanism by which all of the third-party resource servers can outsource resource protection (and potentially discovery) to a central authorization server, as well as ensuring that trust between the authorization server and resource servers

is able to be established by the resource owner in a dynamic, loosely coupled fashion.

Please see the full Resource Set Registration 1.0 Specification [ResourceReg] for a complete description.

2. References

2.1. Normative References

[JSON] Bray, T., "The JavaScript Object Notation (JSON) Data Interchange Format", March 2014, <https://tools.ietf.org/html/rfc7159>.

[OAuth2] Hardt, D., "The OAuth 2.0 Authorization Framework", October 2012, <http://tools.ietf.org/html/rfc6749>.

[ResourceReg] Hardjono, T., Maler, E., Machulak, M., and D. Catalano, "OAuth 2.0 Resource Set Registration Version 1.0.1", December 2015, <https://docs.kantarainitiative.org/uma/rec-oauth-resource-reg-v1_0_1.html>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[UMAcore] Hardjono, T., Maler, E., Machulak, M., and D. Catalano, "User-Managed Access (UMA) Profile of OAuth 2.0 Version 1.0.1", December 2015, <https://docs.kantarainitiative.org/uma/draft-uma-core-v1_0_1.html>.

2.2. Informative References

[OpenIDConnect] Sakimura, N., "OpenID Connect Core 1.0 incorporating errata set 1", November 2014, <http://openid.net/specs/openid-connect-core-1_0.html>.

Authors' Addresses

Thomas Hardjono (editor)
MIT

Email: hardjono@mit.edu

Eve Maler
ForgeRock

Email: eve.maler@forgerock.com

Maciej Machulak
Cloud Identity

Email: maciej.machulak@cloudidentity.co.uk

Domenico Catalano
Oracle

Email: domenico.catalano@oracle.com