Kitten Working Group
Internet Draft
Intended status: Standards Track
Expires: February 1, 2015

K. Zheng
W. Jiang
Intel Corporation
T. Hardjono
T. Yu
MIT Kerberos Consortium

October 25, 2014

Access Token Profile for Kerberos
draft-ietf-kitten-kerb-access-token-01

Abstract

Kerberos provides a pre-authentication framework authenticating client using other authentication mechanisms. Token-preauth defines a token mechanism and also provides common token support facilities for Kerberos. This document extends token-preauth and allows Access Token can be used to request service ticket directly targeting for the service implied by the token.

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), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This Internet-Draft will expire on February 1, 2015.

Copyright Notice

Table of Contents

1. Introduction

This document defines an Access Token profile for Kerberos by extending token-preauth [TKPREAU] and utilizing the provided common token support facilities. This profile allows Access Token to be used to request service ticket directly targeting for the service implied by the token. Assuming an Access Token is granted by a token authority, and then used to request to access a Kerberized service or application server, this profile should be useful, as it allows such integration model between OAuth like system and Kerberos System without requiring modifying either system. This should make sense to the both: 1) for Kerberos, as token based solutions like OAuth 2.0 are more widely used and growing fast in both web and cloud providers, Kerberos should embrace the trend and can accept token input from web frontend to authenticate the token user in the Kerberized backend; 2) for token systems like OAuth 2.0 vendors, as Kerberos is majorly built into enterprise at the backend infrastructure and also used in many important distributed systems like Apache Hadoop, allowing user tokens can be used in the existing Kerberized systems is important for both user experience and the systems.

In token-preauth, two token schemes Identity Token and Access Token are defined. This document uses Access Token scheme or token pattern instead of coupling with concrete token like OAuth 2.0 Access Token. This eliminates the complexities involved in existing token details for the profile, and to deal with such details, token mapping provider defined in token-preauth can be employed to adapt exiting tokens into the ones expected by this profile.

2. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [RFC2119].

This document assumes familiarity with token-preauth and so freely uses terminology and notation from that document.

3. Access Token Profile

This document defines the Access Token profile by extending token-preauth [TKPREAU] and utilizing the provided common token support facilities as follows.

This profile accepts user's Access Token either via input by manually or from web flow, authenticate the user to the KDC using the token via the token pre-authentication mechanism defined in [TKPREAU] in the AS exchange; once the authentication is passed, a service ticket will be returned directly instead of Ticket Granting Ticket.

The client principal name to authenticate and issue service ticket for is determined from the kpn attribute of the token. The client principal MAY not exist if the KDC policy allows.

The service principal name for the service ticket to target is determined from the kau attribute of the token. For Access Token, the value of kau attribute SHOULD be the service principal name, the name SHOULD be validated and exist. Token-preauth uses this attribute to determine the input token is an Access Token or not, and only when it's an Access Token then a service ticket is expected to be returned.

When issuing the service ticket, a derivation of the token will be enriched with all the meaningful attributes for applications and encapsulated into it as Authorization Data using the AD-TOKEN container. Therefore applications can query the token derivation for the attributes and enforce fine-grained authorization as would does in other token profiles.

4. Security Considerations

This document discusses Access Token support for Kerberos utilizing common token facilities provided in token-preauth. When the Bearer Token scheme is used, as it doesn't provide generating and strengthening Client Key and Reply Key facilities, it's not RECOMMENDED that this extension be deployed independently. To protect token from leakage between client and the KDC, we RECOMMEND it SHOULD be deployed together with a pre-authentication mechanism like PKINIT defined in [PKINIT] or OTP defined in [RFC6560], or whatever means that can provide the good enough Armor Key. Sure also, transport layer security like TLS/SSL COULD also be employed to protect token if it's available in the context.

Between client and application servers, as token derivations are encapsulated into service tickets and the later provides the strong enough security channels in Kerberos protocol, there is no need to deploy TLS/SSL to protect tokens as it would in other token profiles.

5. IANA Considerations

TBD

6. References

[RFC4120] Neuman, C., Yu, T., Hartman, S., and K. Raeburn, "The Kerberos Network Authentication Service (V5)", RFC 4120, July 2005.

[RFC6113] Hartman, S. and L. Zhu, "A Generalized Framework for Kerberos Pre-Authentication", RFC 6113, April 2011.

[RFC6749] D. Hardt, Ed., "The OAuth 2.0 Authorization Framework", RFC 6749, October 2012.

[JWT] M. Jones, J. Bradley, N. Sakimura, "JSON Web Token (JWT)", draft-ietf-oauth-json-web-token-22 (work in progress), June 20, 2014.

[TKPREAU] K. Zheng, W. Jiang, T. Hardjono, "Token Pre-Authentication for Kerberos (token-preauth)", draft-ietf-kitten-kerb-token-preauth-01 (work in progress), October 25, 2014.

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

7. Acknowledgments

This initial draft incorporated many important feedbacks from both Greg and Ben Kaduk (MIT) in the early discussion about this mechanism.

Thanks Dey, Avik and Andrew Purtell for the early interesting and confirmation for the prototype of the idea in this direction. And thanks to Xiang Zhong for his initial review and feedback.

Authors' Addresses

Kai Zheng

Intel Corporation

Email: kai.zheng@intel.com

Weihua Jiang

Intel Corporation

Email: weihua.jiang@intel.com

Thomas Hardjono

MIT Kerberos Consortium

Email: hardjono@mit.edu

Tom Yu

MIT Kerberos Consortium

Email: tlyu@mit.edu