

Internet Engineering Task Force  
Internet-Draft  
Updates: [4120](#) (if approved)  
Intended status: Standards Track  
Expires: November 17, 2016

A. Jain  
Georgia Tech  
N. Kinder  
N. McCallum  
Red Hat, Inc.  
May 16, 2016

Authentication Indicator in Kerberos Tickets  
draft-ietf-kitten-krb-auth-indicator-02

## Abstract

This document specifies an extension in the Kerberos protocol [[RFC4120](#)]. It defines a new authorization data type AD-AUTHENTICATION-INDICATOR. The purpose of introducing this data type is to include an indicator of the strength of a client's authentication in the service tickets so that application services can use it as an input into policy decisions.

## 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 November 17, 2016.

## Copyright Notice

Copyright (c) 2016 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

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">2.</a>	Document Conventions . . . . .	<a href="#">2</a>
<a href="#">3.</a>	AD Type Specification . . . . .	<a href="#">2</a>
<a href="#">4.</a>	Security Considerations . . . . .	<a href="#">3</a>
<a href="#">5.</a>	References . . . . .	<a href="#">3</a>
<a href="#">5.1.</a>	Normative References . . . . .	<a href="#">3</a>
<a href="#">5.2.</a>	Informative References . . . . .	<a href="#">4</a>
<a href="#">Appendix A.</a>	ASN.1 Module . . . . .	<a href="#">4</a>
<a href="#">Appendix B.</a>	Acknowledgements . . . . .	<a href="#">4</a>

## [1.](#) Introduction

Kerberos [[RFC4120](#)] allows secure interaction among users and services over a network. It supports a variety of authentication mechanisms using its pre-authentication framework [[RFC6113](#)]. The Kerberos authentication service has been architected to support password based authentication as well as multi-factor authentication using one-time password devices or public key cryptography. Implementations that have pre-authentication mechanisms offering significantly different strengths of client authentication may choose to keep track of the strength of the authentication used as an input into policy decisions.

This document specifies a new authorization data type to convey authentication strength to application services. Elements of this type appear within an AD-CAMMAC [[RFC7751](#)] container.

## [2.](#) Document Conventions

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](#)].

## [3.](#) AD Type Specification

The KDC MAY include the following authorization data element, wrapped in AD-CAMMAC, in initial credentials, and copy it from a ticket-

granting ticket into service tickets:

AD-AUTHENTICATION-INDICATOR 97

Jain, et al.

Expires November 17, 2016

[Page 2]

---

Internet-Draft

Authentication Indicator

May 2016

The corresponding ad-data field contains the DER encoding of the following ASN.1 type:

```
AD-AUTHENTICATION-INDICATOR ::= SEQUENCE OF UTF8String
```

Each UTF8String value is a short string that indicates that a particular set of requirements was met during the initial authentication. These strings are intended to be compared against known values. They are not intended to store structured data. These strings MAY be site-defined strings that do not contain a colon such as the name of the Pre-Authentication mechanism used, or alternatively URIs that reference a Level of Assurance Profile [[RFC6711](#)].

Authorization data elements of type AD-AUTHENTICATION-INDICATOR MUST be included in an AD-CAMMAC container so that their contents can be verified as originating from the KDC. Elements of type AD-AUTHENTICATION-INDICATOR MAY safely be ignored by applications and KDCs that do not implement this element.

#### 4. Security Considerations

Elements of type AD-AUTHENTICATION-INDICATOR are wrapped in AD-CAMMAC containers. AD-CAMMAC supersedes AD-KDC-ISSUED, and allows both application services and the KDC to verify the authenticity of the contained authorization data.

KDC implementations MUST use AD-CAMMAC verifiers as described in the the security considerations of [RFC 7751](#) [[RFC7751](#)] to ensure that AD-AUTHENTICATION-INDICATOR elements are not modified by an attacker. Application servers MUST validate the AD-CAMMAC container before making authorization decisions based on AD-AUTHENTICATION-INDICATOR elements. Application servers MUST NOT make authorization decisions based on AD-AUTHENTICATION-INDICATOR elements which appear outside of AD-CAMMAC containers.

Using multiple strings in AD-AUTHENTICATION-INDICATOR MAY lead to ambiguity when a service tries to make a decision based on the AD-AUTHENTICATION-INDICATOR values. This ambiguity can be avoided if indicator values are always used as a positive indication of certain requirements being met during the initial authentication.

## 5. References

### 5.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/

Jain, et al. Expires November 17, 2016 [Page 3]

---

Internet-Draft Authentication Indicator May 2016

[RFC2119](#), March 1997,  
<<http://www.rfc-editor.org/info/rfc2119>>.

[RFC4120] Neuman, C., Yu, T., Hartman, S., and K. Raeburn, "The Kerberos Network Authentication Service (V5)", [RFC 4120](#), DOI 10.17487/RFC4120, July 2005,  
<<http://www.rfc-editor.org/info/rfc4120>>.

[RFC6113] Hartman, S. and L. Zhu, "A Generalized Framework for Kerberos Pre-Authentication", [RFC 6113](#), DOI 10.17487/[RFC6113](#), April 2011,  
<<http://www.rfc-editor.org/info/rfc6113>>.

[RFC7751] Sorce, S. and T. Yu, "Kerberos Authorization Data Container Authenticated by Multiple Message Authentication Codes (MACs)", [RFC 7751](#), DOI 10.17487/RFC7751, March 2016,  
<<http://www.rfc-editor.org/info/rfc7751>>.

### 5.2. Informative References

[MS-SFU] Microsoft, "Kerberos Protocol Extensions: Service for User and Constrained Delegation Protocol", January 2013,  
<<http://msdn.microsoft.com/en-us/library/cc246071.aspx>>.

[RFC6711] Johansson, L., "An IANA Registry for Level of Assurance (LoA) Profiles", [RFC 6711](#), DOI 10.17487/RFC6711, August 2012, <<http://www.rfc-editor.org/info/rfc6711>>.

[Appendix A.](#) ASN.1 Module

```
KerberosV5AuthenticationIndicators {
    iso(1) identified-organization(3) dod(6) internet(1)
    security(5) kerberosV5(2) modules(4)
    authentication-indicators(9)
} DEFINITIONS EXPLICIT TAGS ::= BEGIN

AD-AUTHENTICATION-INDICATOR ::= SEQUENCE OF UTF8String

END
```

## [Appendix B](#). Acknowledgements

Dmitri Pal (Red Hat)  
Simo Sorce (Red Hat)  
Greg Hudson (MIT)

Jain, et al. Expires November 17, 2016 [Page 4]

---

Internet-Draft Authentication Indicator May 2016

### Authors' Addresses

Anupam Jain  
Georgia Tech  
225 North Ave NW  
Atlanta, GA 30332  
USA

E-Mail: [ajain323@gatech.edu](mailto:ajain323@gatech.edu)

Nathan Kinder  
Red Hat, Inc.  
444 Castro St.  
Suite 500  
Mountain View, CA 94041  
USA

E-Mail: [nkinder@redhat.com](mailto:nkinder@redhat.com)

Nathaniel McCallum

Red Hat, Inc.  
100 East Davie Street  
Raleigh, NC 27601  
USA

EMail: [npmccallum@redhat.com](mailto:npmccallum@redhat.com)