

Network Working Group  
Internet Draft  
Document: [draft-melnikov-ldap-krb-authzid-01.txt](#)

A. Melnikov  
Isode Limited  
November 2006  
Expires in six months

Additional authorization identity syntax for Kerberos-aware Directories

#### Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of 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/lid-abstracts.html>

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

A revised version of this draft document will be submitted to the RFC editor as a Draft Standard for the Internet Community. Discussion and suggestions for improvement are requested. Distribution of this draft is unlimited.

---

Internet DRAFT      Kerberos Authorization Id for LDAP      20 November 2006

## Abstract

This document defines new LDAP authorization identity syntax for Kerberos-aware Directories.

### 1.      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](#). [[KEYWORDS](#)]

### 2.      Authorization Identity Syntax for Kerberos

This document defines a new LDAP [LDAP] authorization identity syntax for Directories that support Kerberos V5 [[KERBEROS](#)]. For example, an LDAP server that implements SASL GSSAPI [[SASL-GSSAPI](#)] mechanism may also support the new syntax defined below.

The following syntax specification uses the augmented Backus-Naur Form (BNF) notation as specified in [[ABNF](#)]. Non-terminals referenced but not defined below are as defined by [[AUTHMECH](#)], [[KERBEROS](#)] and [[UTF-8](#)].

```
authzId                    =/ krbAuthzId

KRBCOLON                  = %x6B %x72 %x62 %x3a ; "krb:"

krbAuthzId                = KRBCOLON krbPrincipal
                          ; kerberos-principal-name-based
                          ; authorization id.

krbRealmDelimiter        = %x40
                          ; '@'

krbComponentDelimiter    = %x2F
                          ; '/'

krbPrincipal              = krbNameComponents
                          [krbRealmDelimiter krbRealm]
```

```
krbNameComponents      = krbNameComponent
                        *(krbComponentDelimiter krbNameComponent)

krbNameComponent        = KerberosString ; *UTF8
                        ; This corresponds to individual
```

Internet DRAFT      Kerberos Authorization Id for LDAP      20 November 2006

```
                        ; "name-string" of "PrincipalName" as defined
                        ; in [KERBEROS].
                        ;
                        ; '/', '\ ' and '@' characters must be escaped
                        ; by prefixing with \, i.e. "\@"

krbRealm                = KerberosString ; *UTF8
                        ; This corresponds to "Realm" as defined in
                        ; [KERBEROS]. The syntax is constrained as
                        ; described in section 6 of [KERBEROS].
                        ;
                        ; '/', '\ ' and '@' characters must be escaped
                        ; by prefixing with \, i.e. "\@"
```

The krbAuthzId choice allows a client to assert an authorization identity of a Kerberos principal when the client doesn't know a corresponding distinguished name for the asserted identity. A krbAuthzId is prefixed with a unique prefix "krb:" which is followed by a Kerberos principal (krbPrincipal). krbPrincipal consists of one or more components (components of "name-string" [[KERBEROS](#)]) that form a principal name followed by an optional Kerberos realm (krbRealm). <<Add an example?>> Before constructing a krbPrincipal each principal name component and the realm MUST be prepared using the "SASLPrep" profile [[SASLPrep](#)] of the "stringprep" algorithm [[RFC3454](#)].

<<Is there a KerberosPrep or does Kerberos use SASLPrep?>>

All the krbNameComponent elements are delimited by the '/' character. The principal name components are separated from the realm by the '@' character. Because of the special meaning of the '/' and the '@' as the delimiters, they are not allowed to be unescaped if used inside of krbNameComponent (see Section 6.2 of [[KERBEROS](#)] for an example) or krbRealm. The '\' character is used as the escape character. The '\' itself has to be escaped.

Note that it is a typical for Kerberos/GSSAPI implementations to use '/' and '@' as the delimiters.

<<An alternative proposal: All the krbNameComponent elements and the realm are separated by Unicode ZERO WIDTH NO-BREAK SPACE character encoded in UTF-8 (%xEF %xBB %xBF). The ZERO WIDTH NO-BREAK SPACE was selected as the delimiter character, as it never appears in any SASLPrep output.

An alternative delimiter character: SOFT HYPHEN (U+00AD)

A. Melnikov

FORMFEED[Page 3]

---

Internet DRAFT      Kerberos Authorization Id for LDAP      20 November 2006

Advantage of the proposal: no escaping mechanism required.  
Disadvantage of the proposal: not easy way to type krbAuthzId on a command line. >>

<<Describe how comparison is to be performed. For the realm part it may or may not be ASCII case sensitive. This is mostly implementation dependent, for example not all implementations support X500 syntax for realms. Some implementations may assume that a realm is a domain and treat it case insensitively. The principal name part is implementation dependent.>>

Note, that name-type element of PrincipalName [[KERBEROS](#)] is not being used in krbPrincipal.

This document doesn't mandate how an LDAP server performs internal mapping of a krbPrincipal to the corresponding distinguished name. For example, an implementation may choose to do an algorithmic mapping ("user1@EXAMPLE.COM" ==> "cn=user1, dc=EXAMPLE, dc=COM"), or perform a search based mapping. The client may use LDAP "Who am I?" Extended Operation [[WHO-AM-I](#)] to discover the resulting distinguished name.

### [3.](#)    Security considerations

<<TBD>>

## [4.](#) References

### [4.1.](#) Normative References

[KEYWORDS] Bradner, "Key words for use in RFCs to Indicate Requirement Levels", [RFC 2119](#), March 1997

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

[AUTHMECH] Harrison, R. (Editor), "Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms", [RFC 4513](#), June 2006.

[ABNF] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", [RFC 4234](#), October 2005.

[UTF-8] Yergeau, F., "UTF-8, a transformation format of ISO 10646",

A. Melnikov

FORMFEED[Page 4]

---

Internet DRAFT      Kerberos Authorization Id for LDAP      20 November 2006

[RFC 3629](#), STD 63, November 2003.

[RFC3454] P. Hoffman, M. Blanchet, "Preparation of Internationalized Strings ("stringprep")," [RFC 3454](#), December 2002.

[SASLPrep] Zeilenga, K., "SASLprep: Stringprep Profile for User Names and Passwords", [RFC 4013](#), February 2005.

### [4.2.](#) Informative References

[SASL-GSSAPI] Melnikov, A., "SASL GSSAPI mechanisms", [draft-ietf-sasl-gssapi](#), work in progress. <<Needs updating>>

[WHO-AM-I] Zeilenga, K., "Lightweight Directory Access Protocol (LDAP) - "Who am I?" Operation", [RFC 4532](#), June 2006.

## [5.](#) Author's Address

Alexey Melnikov

Iside Limited  
5 Castle Business Village  
36 Station Road  
Hampton, Middlesex  
TW12 2BX, United Kingdom

Email: Alexey.Melnikov@isode.com

URI: <http://www.melnikov.ca/>

## 6. Acknowledgments

Thanks to Chris Ridd for providing useful feedback and suggestions.

### Disclaimer of validity

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this

specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at [ietf-ipr@ietf.org](mailto:ietf-ipr@ietf.org).

## Full Copyright Statement

Copyright (C) The Internet Society (2006). This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

## Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.

A. Melnikov

FORMFEED[Page 6]

---

Internet DRAFT      Kerberos Authorization Id for LDAP      20 November 2006

Status of this Memo .....	<a href="#">i</a>
Abstract .....	<a href="#">2</a>
<a href="#">1.</a> Conventions used in this document .....	<a href="#">2</a>
<a href="#">2.</a> Authorization Identity Syntax for Kerberos .....	<a href="#">2</a>
<a href="#">3.</a> Security considerations .....	<a href="#">4</a>
<a href="#">4.</a> References .....	<a href="#">4</a>
<a href="#">4.1.</a> Normative References .....	<a href="#">4</a>
<a href="#">4.2.</a> Informative References .....	<a href="#">5</a>

<a href="#">5.</a>	Author's Address .....	<a href="#">5</a>
<a href="#">6.</a>	Acknowledgments .....	<a href="#">5</a>