

Network Working Group  
Internet-Draft  
Updates: [rfc4120](#) (if approved)  
Intended status: Standards Track  
Expires: April 18, 2013

T. Yu  
MIT Kerberos Consortium  
October 15, 2012

Move Kerberos protocol parameter registries to IANA  
draft-ietf-kitten-kerberos-iana-registries-00

## Abstract

The Kerberos 5 network authentication protocol has several numeric protocol parameters. Most of these parameters are not currently under IANA maintenance. This document requests that IANA take over the maintenance of the remainder of these Kerberos parameters.

## 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 April 18, 2013.

## Copyright Notice

Copyright (c) 2012 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.

Internet-Draft

Kerberos IANA registries

October 2012

## [1.](#) Introduction

The Kerberos 5 network authentication protocol has several numeric protocol parameters. This document requests that IANA take over the maintenance of the Kerberos protocol parameters that are not currently under IANA maintenance. Several instances of number conflicts in Kerberos implementations could have been prevented by having IANA registries for those numbers.

## [2.](#) General registry format

Unless otherwise specified, each Kerberos protocol number registry will have the following fields: "number", "name", "reference", and "comments".

The name must begin with a lowercase letter, and must consist of ASCII letters, digits, and hyphens. Two or more hyphens must not appear directly adjacent to each other. A hyphen must not appear at the end of a name. It is preferred that words in a name be separated by hyphens, and that all of the letters be lowercase.

(These rules are consistent with the lexical rules for an ASN.1 valuereference or identifier. Where the constraints are stricter than the ASN.1 lexical rules, they make it easier to systematically translate the names for use in implementation languages.)

Names for numeric parameter values have no inherent meaning in the Kerberos protocol, but they can guide choices for internal implementation symbol names and for user-visible non-numeric representations. When written in English prose in specifications, or when used as symbolic constants in implementation languages (e.g., C preprocessor macros), it is common to transform the name into all uppercase letters, and possibly to replace hyphens with underscores.

## [3.](#) General registration procedure

This document requests that the IESG establish a pool of Kerberos experts who will manage the Kerberos registries using these guidelines. The IESG may wish to consider including the set of designated IANA experts for existing Kerberos IANA registries as candidates for this pool.

IANA will select an expert from this pool for each registration request. The expert will review the registration request and may approve the registration, decline the registration with comments, or recommend that the registration request should follow a specific

alternative process. The alternative processes that the expert may recommend are the IETF review process and the standards action process.

Initially, the experts reviewers will use a permissive process, generally approving registrations that are architecturally consistent with Kerberos and the protocol parameter in question. Over time, with input from the community, the experts may refine the requirements that registrations are expected to meet. The experts will maintain a current version of these guidelines in a manner that is generally accessible to the entire community. As the guidelines evolve, experts may consider the technical quality of specifications, security impacts of the registrations, architectural consistency, and interoperability impact. Experts may require a publicly available specification in order to make certain registrations.

[ For the individual registries, include "Registrations in this registry are managed by the expert review process [[RFC5226](#)] or in exceptional cases by IESG approval. See section x for guidelines for the experts to be used with this registry." ]

#### [4.](#) Integer assignments

Names for integer assignments must be unique across all Kerberos integer parameter registries. This is normally accomplished by including a name prefix that identifies the registry.

Assignments for integers parameters will follow the general registration procedure outlined above, except as otherwise noted in the section that contains the description of the parameter. Kerberos integer parameters take on signed 32-bit values (-2147483648 to 2147483647). Negative values are for private or local use.

##### [4.1.](#) Address types

Address types historically align with numeric constants used in the Berkeley sockets API. Future address type assignments should conform to this historical practice when possible. The name prefix for address types is "addrtype-".

#### [4.2.](#) Authorization data types

The name prefix for authorization data types is "ad-".

Yu

Expires April 18, 2013

[Page 3]

Internet-Draft

Kerberos IANA registries

October 2012

#### [4.3.](#) Error codes

Assignments for error codes require standards action due to their scarcity: assigning error codes greater than 127 could require significant changes to certain implementations. The name prefixes for error codes are "kdc-err-", "krb-err", or "krb-ap-err".

#### [4.4.](#) Key usages

Key usages are unsigned 32-bit integers (0 to 4294967295). Zero is reserved and may not be assigned.

The name prefix for key usages is "ku-".

#### [4.5.](#) Name types

The name prefix for name types is "nt-".

number	name	reference	comment
0	nt-unknown	<a href="#">RFC4120</a>	Name type not known
1	nt-principal	<a href="#">RFC4120</a>	Just the name of the principal as in DCE, or for users
2	nt-srv-inst	<a href="#">RFC4120</a>	Service and other unique instance (krbtgt)
3	nt-srv-hst	<a href="#">RFC4120</a>	Service with host name as instance (telnet,

				rcommands)
4	nt-srv-xhst	<a href="#">RFC4120</a>		Service with host as remaining components
5	nt-uid	<a href="#">RFC4120</a>		Unique ID
6	nt-x500-principal	<a href="#">RFC4120</a>		Encoded X.509 Distinguished name [ <a href="#">RFC2253</a> ]
7	nt-smtp-name	<a href="#">RFC4120</a>		Name in form of SMTP email name (e.g., user@example.com)
10	nt-enterprise	<a href="#">RFC4120</a>		Enterprise name - may be mapped to principal name
11	nt-wellknown	<a href="#">RFC6111</a>		Well-known principal name
12	nt-srv-hst-domain	<a href="#">RFC5179</a>		Domain-based names
+-----+-----+-----+-----+-----+				

#### [4.6.](#) Pre-authentication and typed data

The name prefix for pre-authentication type numbers is "pa-". The name prefix for typed data numbers is "td-". Pre-authentication and typed data numbers are in the same registry, but a pre-authentication number may be also be assigned to a related typed data number.

### [5.](#) Named bit assignments

Assignments for named bits require standards action, due to their scarcity: assigning bit numbers greater than 31 could require significant changes to implementations. Names for named bit assignments must be unique within a given named bit registry, and typically do not have name prefixes that identify which registry they belong to.

#### [5.1.](#) AP-REQ options

#### [5.2.](#) KDC-REQ options

#### [5.3.](#) Ticket flags

## 6. Contributors

Sam Hartman proposed the text of the expert review guidelines. Love Hornquist Astrand wrote a previous document ([draft-lha-krb-wg-some-numbers-to-iana-00](#)) with the same goals as this document.

## 7. Security Considerations

Assignments of new Keberos protocol parameter values can have security implications. In cases where the assignment policy calls for expert review, the reviewer is responsible for evaluating whether adequate documentation exists concerning the security considerations for the requested assignment. For assignments that require IETF review or standards action, the normal IETF processes ensure adequate treatment of security considerations.

## 8. IANA Considerations

This document requests that IANA create several registries for Keberos protocol parameters. This document also requests that IANA modify several existing registries of Kerberos protocol parameters.

Yu

Expires April 18, 2013

[Page 5]

---

Internet-Draft

Kerberos IANA registries

October 2012

This document requests that IANA modify the existing "Pre-authentication data and typed data" registry to contain an additional reference to this document, and to transform existing names in that registry to the lowercase-and-hyphens style.

## 9. References

### 9.1. Normative References

- [RFC3961] Raeburn, K., "Encryption and Checksum Specifications for Kerberos 5", [RFC 3961](#), February 2005.
- [RFC4120] Neuman, C., Yu, T., Hartman, S., and K. Raeburn, "The Kerberos Network Authentication Service (V5)", [RFC 4120](#),

July 2005.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", [BCP 26](#), [RFC 5226](#), May 2008.

## [9.2](#). Informative References

[RFC1510] Kohl, J. and B. Neuman, "The Kerberos Network Authentication Service (V5)", [RFC 1510](#), September 1993.

## Author's Address

Tom Yu  
MIT Kerberos Consortium  
77 Massachusetts Ave  
Cambridge, Massachusetts  
USA

Email: [tlyu@mit.edu](mailto:tlyu@mit.edu)