NETWORK WORKING GROUP	N. Williams	
Internet-Draft	Sun	
Intended status: Standards Track	April 02, 2009	
Expires: October 4, 2009		

TOC

Namespace Considerations and Registries for GSS-API Extensions
draft-ietf-kitten-gssapi-extensions-iana-06.txt

Status of this Memo

Copyright Notice

Abstract

This document describes the ways in which the GSS-API may be extended and directs the creation of an IANA registry for various GSS-API namespaces.

Table of Contents

---

1. Conventions used in this document

TOC

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 [RFC2119] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.).

---

2. Introduction

TOC

There is a need for private-use and mechanism-specific extensions to the Generic Security Services Application Programming Interface (GSS-API). As such extensions are designed and standardized (or not), both at the IETF and elsewhere, there is a non-trivial risk of namespace pollution and conflicts. To avoid this we set out guidelines for extending the GSS-API and direct the creation of an IANA registry for GSS-API namespaces.
Registrations of individual items and sub-namespaces are allowed. Each sub-namespace may provide different rules for registration, e.g., for mechanism-specific and private-use extensions.

---

3. Extensions to the GSS-API

TOC

Extensions to the GSS-API can be categorized as follows:

- *Abstract API extensions
- *Implementation-specific
- *Mechanism-specific
- *Language binding-specific

Extensions to the GSS-API may be purely semantic, without effect on the GSS-API's namespaces. Or they may introduce new functions, constants, types, etc...; these clearly affect the GSS-API namespaces. Extensions that affect the GSS-API namespaces should be registered with the IANA as described herein.

---

4. Generic GSS-API Namespaces

TOC

The abstract API namespaces for the GSS-API are:

- *Type names
- *Function names
- *Constant names for various types
- *Constant values for various types
- *Name types (OID, type name and syntaxes)

Additionally we have namespaces associates with the OBJECT IDENTIFIER (OID) type. The IANA already maintains a registry of such OIDs:

- *Mechanism OIDs
- *Name Type OIDs

TOC

5. Language Binding-Specific GSS-API Namespaces

Language binding specific namespaces include, among others:

- *Header/interface module names
- *Object classes and/or types
- *Methods and/or functions
- *Constant names
- *Constant values

---

6. Extension-Specific GSS-API Namespaces

TOC

Extensions to the GSS-API may create additional namespaces. See Section 8.2 (Registration Maintenance Guidelines).

---

7. Registration Form

TOC

Registrations for GSS-API namespaces SHALL take the following form:

Registration Field	Possible Values	Description
Registration type	'Instance', 'Sub-Namespace'	Indicates whether this entry reserves a given symbol name (and possibly, constant value), or whether it reserves an entire sub-namespace (the name is a pattern) or constant value range.
Bindings	'Generic', 'C-bindings', 'Java', 'C#', <programming language name>	Indicates the name of the programming language that this registration involves, or, if 'Generic', that this is an entry for the generic abstract GSS-API (i.e., not specific to any programming language).
Object Type	'Data-Type', 'Function', 'Method', 'Integer', 'String', 'OID',	Indicates the type of the object whose symbolic name or constant value this entry registers. The possible values of this field

	'Context-Flag', 'Name-Type', 'Macro', 'Header-File-Name', 'Module-Name', 'Class', etcetera	depend on the programming language in question, therefore they are not all specified here.
Symbol Name/ Prefix	<Symbol name or name pattern>	The name of a symbol or symbol sub-namespace being registered. See Section 8.2.1 (Sub-Namespace Symbol Pattern Matching)
Binding of	<Name of abstract API element of which this object is a binding>	If the registration is for a specific language binding of the GSS-API, then this names the abstract API element of which it is a binding (OPTIONAL).
Constant Value/Range	<Constant value> or <constant value range>	The value of the constant named by the <Symbol Name/Prefix>. This field is present only for Instance and Sub-namespace registrations of Constant object types.
Description	<Text>	Description of the registration. Multiple instances of this field may result (see Section 8.2.3 (Change Control)).
Registration Rules	Values from [RFC5226] (Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs," May 2008.), such as 'IESG Approval', 'Expert Review', 'First Come First Served', 'Private Use', etcetera.	Describes the rules for allocation of items that fall in this sub-namespace, for entries with Registration Type of Sub-namespace (OPTIONAL). For private use sub-namespaces the submitter MUST provide the e-mail address of a responsible contact.
Reference	<Reference>	Reference to document that describes the registration, if any (OPTIONAL). Multiple instances of this field are allowed, with one reference each.
Expert Reviewer	<Name of expert reviewers, possibly WG names>	OPTIONAL, see Section 8.2.2 (Expert Reviews of Individual Submissions). Multiple instances of this field

		are allowed, with one expert reviewer per-instance.
Expert Review Notes	<Notes from the expert review>	Expert reviewers may request that some comments be included with the registration, e.g., regarding security considerations of the registered extension.
Status	'Registered', 'Obsoleted'	Status of the registration.
Obsoleting Reference	<Reference>	Reference to document, if any, that obsoletes this registration. Multiple instances of this field are allowed, with one reference each. (OPTIONAL)

The IANA should create a single GSS-API namespace registry, or multiple registries, one for symbolic names and one for constant values, and/or it may create a registry per-programming language, at its convenience. Entries in these registries should consist of all the fields from their corresponding registration entries.
Entries should be sorted by: registration type, progamming language, object type, and symbol name/pattern.

---

8. IANA Considerations

TOC

This document deals with IANA considerations throughout. Specifically it creates a single registry of various kinds of things, thought the IANA may instead create multiple registries each for one of those kinds of things. Of particular interest may be that IANA will now be the registration authority for the GSS-API name type OID space.

8.1. Initial Namespace Registrations

TOC

Initial registry content corresponding to the items defined in [RFC2743] (Linn, J., “Generic Security Service Application Program Interface Version 2, Update 1,” January 2000.), [RFC2744] (Wray, J., “Generic Security Service API Version 2 : C-bindings,” January 2000.), [RFC2853] (Kabat, J. and M. Upadhyay, “Generic Security Service API Version 2 : Java Bindings,” June 2000.), [RFC1964] (Linn, J., “The Kerberos Version 5 GSS-API Mechanism,” June 1996.) and [RFC4121] (Zhu, L., Jaganathan, K., and S. Hartman, “The Kerberos Version 5 Generic Security Service Application Program Interface (GSS-API) Mechanism: Version 2,” July 2005.) and others will be supplied during the IANA

review portion of the RFC publishing process. The KITTEN WG chairs MUST indicate that such content has been reviewed by the WG and that there is WG consensus that the entries are in agreement with those RFCs.

8.2. Registration Maintenance Guidelines

TOC

Standards-Track RFCs can create new items with any non-conflicting Symbol Name/Prefix value for this registry by virtue of IESG approval to publish as a Standards-Track RFC -- that is, without additional expert review.
Standards-Track RFCs can mark existing entries as obsolete, and can even create conflicting entries if explicitly stated (the IESG, of course, should review conflicts carefully, and may reject them).
IANA shall also consider submissions from individuals, and via Informational and Experimental RFCs, subject to Expert Review. IANA SHALL allow such registrations if a) they are not conflicting, b) provided that the registration is for object types other than Context-Flags, and c) subject to expert review. Guidelines for expert reviews are given below.

8.2.1. Sub-Namespace Symbol Pattern Matching

TOC

Sub-namespace registrations must provide a pattern for matching symbols for which the sub-namespace's registration rules apply. The pattern consists of a string with the following special tokens:

'', meaning "match any string."

*"%m", meaning "match any mechanism family short-hand name."

*"%i", meaning "match any implementor vanity short-hand name."

For example, "GSS_%m_*" matches "GSS_krb5_foo" since "krb5" is a common short-hand for the Kerberos V GSS-API mechanism [RFC1964] (Linn, J., “The Kerberos Version 5 GSS-API Mechanism,” June 1996.). But "GSS_%m_*" does not match "GSS_foo_bar" unless "foo" is asserted to be a short-hand for some mechanism.

8.2.2. Expert Reviews of Individual Submissions

TOC

Expert review selection SHALL be done as follows. If, at the time that the IANA receives an individual submission for registration in this

registry, there is are any IETF Working Groups chartered to produce GSS-API-related documents, then the IANA SHALL ask the chairs of such WGs to be expert reviewers or to name one. If there are no such WGs at that time, then the IANA SHALL ask past chairs of the KITTEN WG and the author/editor of this RFC to act as expert reviewers or name an alternate.

Expert reviewers of individual registration submissions with Registration Type == Sub-namespace should check that the registration request has a suitable description (which need not be sufficiently detailsed for others to implement) and that the Symbol Name/Prefix is sufficiently descriptive of the purpose of the sub-namespace or reflective of the name of the submitter or associated company.

Expert reviewers of individual registration submissions with Registration Type == Instance should check that the Symbol Name falls under a sub-namespace controlled by the submitter. Registration of such entries which do not fall under such a sub-namespace may be allowed provided that they correspond to long existing non-standard extensions to the GSS-API and this can be easily checked or demonstrated, otherwise IESG Protocol Action is REQUIRED (see previous section). Also, reviewers should check that any registration of constant values have a detailed description that is suitable for other implementors to reproduce, and that they don't conflict with other usages or are otherwise dangerous in the reviewers estimation.

Expert reviewers should review impact on mechanisms, security and interoperability, and may reject or annotate registrations which can have mechanism impact that requires IESG protocol action. Consider, for example, new versions of GSS_Init_sec_context() and/or GSS_Accept_sec_context which have new input and/or output parameters which imply changes on the wire or in behaviour that may result in interoperability issues. A reviewer could choose to add notes to the registration describing such issues, or the reviewer might conclude that the danger to Internet interoperability is sufficient to warrant rejecting the registration.

8.2.3. Change Control

TOC

Registered entries may be marked obsoleted using the same expert review process as for registering entries. Obsoleted entries are not, however, to be deleted, but merely marked having Obsoleted Status. Note that entries may be created as obsoleted to record the fact that the given symbol(s) have been used before, even though continued use of them is discouraged.

Registered entries may also be updated in two other ways: additional references, obsoleting references, and descriptions may be added.

All changes are subject to expert review. The submitter of a change request need not be the same as the original submitter.

Registrations may be modified by addtion, but under no circumstance may any fields be modified except for the Status field.
The IANA SHALL add a field describing the date that a an addition or modification was made, and a description of the change.

9. Security Considerations

TOC

General security considerations relating to IANA registration services apply; see [RFC5226] (Narten, T. and H. Alvestrand, “Guidelines for Writing an IANA Considerations Section in RFCs,” May 2008.).
Also, expert reviewers should look for and may document security related issues with submitters' GSS-API extensions, to the best of the reviewers' ability given the information furnished by the submitter. Reviewers may add comments regarding their limited ability to review a submission for security problems if the submitter is unwilling to provide sufficient documentation.

10. References

TOC

10.1. Normative References

TOC

[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC5226]	Narten, T. and H. Alvestrand, “Guidelines for Writing an IANA Considerations Section in RFCs,” BCP 26, RFC 5226, May 2008 (TXT).

10.2. Informative References

TOC

[RFC1964]	Linn, J., “The Kerberos Version 5 GSS-API Mechanism,” RFC 1964, June 1996 (TXT).
[RFC2743]	Linn, J., “Generic Security Service Application Program Interface Version 2, Update 1,” RFC 2743, January 2000 (TXT).
[RFC2744]	Wray, J., “Generic Security Service API Version 2 : C-bindings,” RFC 2744, January 2000 (TXT).
[RFC2853]	Kabat, J. and M. Upadhyay, “Generic Security Service API Version 2 : Java Bindings,” RFC 2853, June 2000 (TXT).

[RFC4121]	Zhu, L., Jaganathan, K., and S. Hartman, “The Kerberos Version 5 Generic Security Service Application Program Interface (GSS-API) Mechanism: Version 2,” RFC 4121, July 2005 (TXT).

Author's Address

TOC

	Nicolas Williams
	Sun Microsystems
	5300 Riata Trace Ct
	Austin, TX 78727
	US
Email:	Nicolas.Williams@sun.com