        Namespace Considerations and Registries for GSS-API Extensions
              draft-ietf-kitten-gssapi-extensions-iana-10.txt

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.

Status of This Memo

Copyright Notice

Table of Contents

[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 [[RFC2119](#)].

[2](#). Introduction

   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

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

   o Abstract API extensions

o Implementation-specific

o Mechanism-specific

o 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**

The abstract API namespaces for the GSS-API are:

o Type names

o Function names

o Constant names for various types

o Constant values for various types

o 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:

o Mechanism OIDs

o Name Type OIDs

[5](#). **Language Binding-Specific GSS-API Namespaces**

Language binding specific namespaces include, among others:

o Header/interface module names

o Object classes and/or types

o Methods and/or functions

o Constant names

o Constant values

6. Extension-Specific GSS-API Namespaces

Extensions to the GSS-API may create additional namespaces. See
Section 8.2.

7. Registration Form

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

Registration Field	Possible Values	Description
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).
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.
Object Type	<Symbol> defined by the binding language (for example 'Data-Type', 'Function', 'Method', 'Integer', 'String', 'OID', 'Context-Flag', 'Name-Type', 'Macro', 'Header-File-Name', 'Module-Name', 'Class')	Indicates the type of the object whose symbolic name or constant value this entry registers. The possible values of this field 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
Binding of	<Name of abstract	If the registration is for a
	API element of	specific language binding of
	which this object	the GSS-API, then this names
	is a binding>	the abstract API element of
		which it is a binding
		(OPTIONAL).
Constant	<Constant value> or	The value of the constant
Value/Range	<constant value	named by the <Symbol
	range>	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).
Registration	<Reference> to an	Describes the rules for
Rules	IANA registration	allocation of items that
	Policy defined in	fall in this sub-namespace,
	[RFC5226] (or an	for entries with
	RFC that updates	Registration Type of Sub-
	it), for instance	namespace (OPTIONAL). For
	'IESG Approval',	private use sub-namespaces
	'Expert Review',	the submitter MUST provide
	'First Come First	the e-mail address of a
	Served', 'Private	responsible contact. If
	Use'.	this field is not specified
		for a sub-namespace, the
		default registration rules
		specified in Section 8.2
		apply.
Reference	<Reference>	Reference to a document that
		describes the registration,
		if any (OPTIONAL). Multiple
		instances of this field are
		allowed, with one reference
		each.
Expert	<Name of expert	OPTIONAL, see Section 8.2.2.
Reviewer	reviewers, possibly	Multiple instances of this

	WG names>	field are allowed, with one expert reviewer per-instance. Leave this field blank when requesting a registration. It will be filled in by the Expert who reviews the registration.
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' or 'Obsoleted'	Status of the registration.
Obsoleting Reference	<Reference>	Reference to a 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: programming language, registration type, object type, and symbol name/pattern.

8. IANA Considerations

This document deals with IANA considerations throughout. Specifically it creates a single registry of various kinds of things, though 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

   Initial registry content corresponding to the items defined in
   [RFC2743], [RFC2744], [RFC2853], [RFC1964] and [RFC4121] and others
   will be supplied during the IANA review portion of the RFC publishing
   process. [[Note to RFC Editor: Delete the following sentence before
   publication:]] 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.

8.1.1. Example registrations

   In order to sanity check recommended IANA registration templates,
   this section registers several entries.

Registration Field	Possible Values
Bindings	C-bindings
Registration type	Instance
Object Type	Function
Symbol Name	gss_init_sec_context
Binding of	GSS_Init_sec_context
Constant Value/Range	N/A
Description	Create a security context by initiator
Registration Rules	N/A
Reference	RFC 2744
Expert Reviewer	Kitten WG
Expert Review Notes	
Status	Registered
Obsoleting Reference	N/A

Registration Field	Possible Values
Bindings	C-bindings
Registration type	Instance
Object Type	Function
Symbol Name	gss_accept_sec_context
Binding of	GSS_Accept_sec_context
Constant Value/Range	N/A
Description	Accept a security context from initiator
Registration Rules	N/A
Reference	RFC 2744
Expert Reviewer	Kitten WG
Expert Review Notes	
Status	Registered
Obsoleting Reference	N/A

```
+-------------------+---------------------------------------------+
| Registration Field | Possible Values                            |
+-------------------+---------------------------------------------+
| Bindings          | C-bindings                                  |
+-------------------+---------------------------------------------+
| Registration type | Instance                                    |
+-------------------+---------------------------------------------+
| Object Type       | Context-Flag                                |
+-------------------+---------------------------------------------+
| Symbol Name       | GSS_C_DELEG_FLAG                            |
+-------------------+---------------------------------------------+
| Binding of        | deleg_state or deleg_req_flag               |
+-------------------+---------------------------------------------+
| Constant          | 1                                           |
| Value/Range       |                                             |
+-------------------+---------------------------------------------+
| Description       | On output (if set): Delegated credentials   |
|                   | are available via the delegated_cred_handle |
|                   | parameter of GSS_Accept_sec_context.  On    |
|                   | input (if set): With the call to            |
|                   | GSS_Init_sec_context, delegate credentials  |
|                   | to the acceptor.                            |
+-------------------+---------------------------------------------+
| Registration Rules | N/A                                        |
+-------------------+---------------------------------------------+
| Reference         | RFC 2744                                    |
+-------------------+---------------------------------------------+
| Expert Reviewer   | Kitten WG                                   |
+-------------------+---------------------------------------------+
| Expert Review     |                                             |
| Notes             |                                             |
+-------------------+---------------------------------------------+
| Status            | Registered                                  |
+-------------------+---------------------------------------------+
| Obsoleting        | N/A                                         |
| Reference         |                                             |
+-------------------+---------------------------------------------+
```

8.2. Registration Maintenance Guidelines

   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**

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:

o '*', meaning "match any string."

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

o "%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].
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**

[[The following paragraph should be deleted from the document before
publication, as it will not age well. It should be moved to the
shepherding write-up.]]

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 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 doesn't need to be
sufficiently detailed 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

Registered entries may be marked obsoleted using the same expert
review process as for registering new 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, except for changes to
registrations in a sub-namespace which are subject to the rules of
the relevant sub-namespace. The submitter of a change request need
not be the same as the original submitter.

Registrations may be modified by addition, but under no circumstance
may any fields be modified except for the Status field or Contact
Address, or to correct for transcription errors in filing or
processing registration requests.

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

   General security considerations relating to IANA registration
   services apply; see [RFC5226].

   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

10.1. Normative References

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

   [RFC2743] Linn, J., "Generic Security Service Application Program
              Interface Version 2, Update 1", RFC 2743, January 2000.

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

10.2. Informative References

   [RFC1964] Linn, J., "The Kerberos Version 5 GSS-API Mechanism", RFC
              1964, June 1996.

   [RFC2744] Wray, J., "Generic Security Service API Version 2 :
              C-bindings", RFC 2744, January 2000.

   [RFC2853] Kabat, J. and M. Upadhyay, "Generic Security Service API
              Version 2 : Java Bindings", RFC 2853, June 2000.

   [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.

Authors' Addresses

   Nicolas   Williams
   Cryptonector LLC

   Email: nico@cryptonector.com

   Alexey Melnikov
   Isode Ltd
   5 Castle Business Village
   36 Station Road
   Hampton, Middlesex TW12 2BX
   UK

   Email: Alexey.Melnikov@isode.com