General Area
Internet-Draft
Updates: 5226 (if approved)
Intended status: Standards Track
Expires: July 31, 2010

O. Gudmundsson
Shinkuro Inc.
S. Rose
NIST

January 27, 2010

Definitions for expressing standards requirements in IANA registries.
draft-ogud-iana-protocol-maintenance-words-03

Abstract

RFC 2119 defines words that are used in IETF standards documents to indicate standards compliance. These words are fine for defining new protocols, but there are certain deficiencies in using them when it comes to protocol maintainability. Protocols are maintained by either updating the core specifications or via changes in protocol registries.

For example, security functionality in protocols often relies upon cryptographic algorithms that are defined in external documents. Cryptographic algorithms have a limited life span, and new algorithms regularly phased in to replace older algorithms.

This document proposes standard terms to use in protocol registries and possibly in standards track and informational documents to indicate the life cycle support of protocol features and operations.

This Internet-Draft will expire on July 31, 2010.

Copyright Notice

Table of Contents

1. Introduction 4
1.1. Implementation vs. Operations requirements 4
2. Terminology 5
3. Proposed requirement words for IANA protocol registries 5
3.1. MANDATORY 5
3.2. DISCRETIONARY 5
3.3. OBSOLETE 6
3.4. ENCOURAGED 6
3.5. DISCOURAGED 6
3.6. RESERVED 7
3.7. AVAILABLE 7
4. Protocol Registry Maintenance 7
5. Example registry 8
6. Security Considerations 8
7. IANA considerations 9
8. References 9
8.1. Normative References 9
8.2. Informative References 9
Authors' Addresses 9

1. Introduction

The RFC series have been the main way to define Internet protocols and publish lists of related protocol parameters. RFC 3232 [RFC3232] replaced the original document centered process with on-line protocol registries maintained by IANA. In many cases these registries are "write-once" i.e. new things are added; in other cases the requirements of a protocol implementation changes over time. This document is aimed at the second case.

This document is motivated by the experiences of the editors in trying to maintain registries for DNS and DNSSEC. For example, DNS defines a registry for hash algorithms used for a message authentication scheme called TSIG [RFC2845], the first entry in that registry was for HMAC-MD5. The DNSEXT working group decided to try to decrease the number of algorithms listed in the registry and add a column to the registry listing the requirements level for each one. Upon reading that HMAC-MD5 was tagged as "OBSOLETE" a firestorm started. It was interpreted as the DNS community making a statement on the status of HMAC-MD5 for all uses. While the document was definitely overreaching in its specification, the point remained there was no standard way to tag different requirements levels in protocol registries.

In the security community there has been some attempts to indicate emerging and retiring algorithms by adding + or - to RFC 2119 words RFC 4835 [RFC4835], SHOULD+ is to be interpreted as "SHOULD for now, expected to be MUST soon". MUST- indicates that the currently required algorithm or feature might be retired sometime in the near future. This has traditionally been accomplished by adding a terminology section to each document. A now expired draft (draft-hoffman-additional-key-words) attempted to establish these additions as new keywords but was never fully adopted. This document attempts to revive this effort. This document adds to and updates the labels defined in RFC 5226 [RFC5226] as well.

In this document when we say "registry" we mean both "IANA registry" and RFC's specifying (or updating) a protocol and its parameters.

1.1. Implementation vs. Operations requirements

It is common that before a new technology is considered "useful" it has to gain widespread deployment. Thus it makes sense to have different levels of RFC 2119 words requirement on implementations than on operations.

In a world of protocol maintenance when something is being 'retired' it is nice if operations can easily migrate to a newer functionality.

This document includes certain extra requirements on implementations during the phase-out of a functionality.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", and "MAY" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. Proposed requirement words for IANA protocol registries

The words below are expected to be in a separate column in the Registries indicating what support implementations are expected to provide for each functionality.

3.1. MANDATORY

This is the strongest requirement and for an implementation to ignore it there MUST be a valid and serious reason.

Implementations: To be considered compliant, all implementations MUST support this registry entry.
Operations: To be considered compliant, operations MUST use at least one of the mandatory entries.
Note 1: There can be more than one MANDATORY requirement.
Note 2: The requirement applies only to new or future implementations on the day the requirement is released. In many cases existing implementations can become compliant via software upgrade or point release.

3.2. DISCRETIONARY

Implementations: Any implementation MAY or MAY NOT support this entry in the protocol registry. The presence or omission of this MUST NOT be used to judge implementations on standards compliance.
Operations: Any use of this registry entry in operation is supported, ignoring or rejecting requests using this protocol component MUST NOT be used as bases for asserting lack of compliance.
Note 1: Discretionary is taken to mean that the given functionality MAY or MAY NOT be supported by an implementation or a given operation MAY or MAY NOT be used.

3.3. OBSOLETE

Implementations: New implementations SHOULD NOT support this functionality.
Operations: Any use of this functionality in operation MUST be phased out.
Note: This is the most dangerous term of the requirements words as it is easy to read too much into this term. The intent is to express the following:
* This functionality is not needed/desired anymore by the given protocol. This is not to say that this particular functionality should be obsoleted by other protocols that use the same (or similar) functionality.

3.4. ENCOURAGED

This word is added to the registry entry when new functionality is added and before it is safe to rely solely on it. Protocols that have the ability to negotiate capabilities MAY NOT need this state. This is similar in spirit to the use of SHOULD+ as defined in certain RFC's (such as RFC 4835 [RFC4835])
Implementations: This functionality SHOULD be supported by implementations.
Operations: This functionality SHOULD NOT be immediately deployed as part of normal operations. This functionality SHOULD be tested in a controlled environment to measure the quality and readiness of the functionality and gain operational experience. Operators can expect functionality marked ENCOURAGED to become MANDATORY at some point in the future unless a significant problem is encountered during early deployments.
Note1: In broadcast protocols like BGP and DNS there is no way for an originator of a message to know the capabilities of all recipients. In these cases the requirement for support ought to be placed on implementations before the functionality is used in operations to guarantee maximum acceptance of the messages.
Note2: In some cases this requires having both "new" and "old" algorithms in use at the same time. In this case the new functionality can be used before a high percentage of deployment of the new functionality has taken place.
Note3: In protocols that negotiate which functionality to use, there is no reason to place different requirement on operations other than list of accepted functionality SHOULD contain at least one MANDATORY functionality.

3.5. DISCOURAGED

This requirement is placed on an existing function that is being phased out. This is similar in spirit to both MUST- and SHOULD- as

defined and used in certain RFC's such as RFC 4835 [RFC4835]

Implementations: Implementations SHOULD support this functionality, and SHOULD provide features to migrate to a MANDATORY functionality. The use of this functionality SHOULD NOT be used as default behavior.
Operations: Operations SHOULD phase out any use of this functionality.
Note: This is the strongest signal to the community that this functionality is no longer considered best practice. Some time after the functionality enters this state, it will migrate to OBSOLETE.

3.6. RESERVED

Sometimes there is a need to reserve certain values to avoid problems such as values that have been used in implementations but were never formally registered. In other cases reserved values are magic numbers that may be used in the future as escape valves if the number space becomes too small.
Implementations: Implementations MUST NOT use any RESERVED values for implementation specific processing.
Operations: MUST NOT be used, any implementation in use that uses this code SHOULD be upgraded/retired.

3.7. AVAILABLE

This is a value that can be allocated by IANA at any time.
Implementations: Implementations SHOULD NOT use these values for implementation specific processing.
Operations: Any implementation claiming to know the meaning of this unallocated code MUST NOT be used.

4. Protocol Registry Maintenance

In theory the process to change the status of a protocol field should be the same as reserving a new field. In practice this is going to be burdensome, as there is a chance the IESG will have to process many documents that are simply saying "Value X in Registry Y is now Mandatory" (or similar).

For this reason we propose that it be possible to make reservations and have a change in that reservation to take place at a defined date in the future. This is a change to the static labels defined in Section 4 of [RFC5226] to include a defined lifetime for certain registry entries. For example, a document could say:

Value X in registry Y is "ENCOURAGED". On June 1st 2020 this value is to become "MANDATORY".

or Value X in registry Y is "DISCOURAGED". On June 1st 2020 this value is to become "OBSOLETE".

or Value X in registry Y is "RESERVED" until June 1st 2020 when this value becomes "AVAILABLE".

5. Example registry

This is an example registry for an example protocol FOO that uses an encrypted channel for messages. The algorithms listed here are only for illustration uses.

FOO

Value	Algorithm name	Requirement	References
0		RESERVED	RFCFOO
1	ROT-13	OBSOLETE	RFCFOO, RFCrot13
2	DES	DISCOURAGED	RFCFOO, RFCdes
3	BlowFish	MANDATORY	RFCblowfish, RFCrot13
4		RESERVED until 2022	RFCrot13
5	AES	Encouraged	RFCFOOaes
6	Enigma	DISCOURAGED, OBSOLETE in Jan 2012	RFCFOO, RFC-Enigma
7 - 255		Available	RFCFOO

Allocation policy for FOO: any RFC published on April 1'st.

Table 1

6. Security Considerations

This document specifies a set of terms to indicate the status of features in protocol implementations and operations. It is not meant to be a discussion on feature or operation superiority or provide a means to measure the usefulness of a feature. It is hoped that by extending the RFC 2119 words to be more applicable for protocol maintenance, the overall security of the Internet is improved.

7. IANA considerations

This document does set rules for registrations of compliance requirements in IANA registries.

This document places requirement that IANA be able to update registires on specific dates. As none of these action is time critical, IANA can perform the actions within a 2 week window of the action specified. Any action saying "Month year" should be interpreded to be applicable on the 15'th of the month, similarly any action say only the year is applicable on June 30'th that year.

8. References

8.1. Normative References

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

[RFC4835] Manral, V., "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 4835, April 2007.

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

8.2. Informative References

[RFC2845] Vixie, P., Gudmundsson, O., Eastlake, D., and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", RFC 2845, May 2000.

[RFC3232] Reynolds, J., "Assigned Numbers: RFC 1700 is Replaced by an On-line Database", RFC 3232, January 2002.

Authors' Addresses

Olafur Gudmundsson
Shinkuro Inc.
4922 Fairmont Avenue, Suite 250
Bethesda, MD 20814
USA

Email: ogud@ogud.com

Scott Rose
NIST
100 Bureau Dr.
Gaithersburg, MD 20899
USA

Phone: +1-301-975-8439
Email: scottr.nist@gmail.com