Network Working Group
Request for Comments: 4289
BCP: 13
Obsoletes: 2048
Category: Best Current Practice

N. Freed
Sun Microsystems
J. Klensin

December 2005

Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures

Status of This Memo

This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

This document specifies IANA registration procedures for MIME external body access types and content-transfer-encodings.

Table of Contents

1. Introduction 2
2. External Body Access Types 3
2.1. Registration Requirements 3
2.1.1. Naming Requirements 3
2.1.2. Mechanism Specification Requirements 3
2.1.3. Publication Requirements 4
2.1.4. Security Requirements 4
2.2. Registration Procedure 4
2.2.1. Present the Access Type to the Community 4
2.2.2. Access Type Reviewer 4
2.2.3. IANA Registration 5
2.3. Location of Registered Access Type List 5
2.4. IANA Procedures for Registering Access Types 5
3. Transfer Encodings 5
3.1. Transfer Encoding Requirements 6
3.1.1. Naming Requirements 6
3.1.2. Algorithm Specification Requirements 6
3.1.3. Input Domain Requirements 6
3.1.4. Output Range Requirements 6
3.1.5. Data Integrity and Generality Requirements 7
3.1.6. New Functionality Requirements 7
3.1.7. Security Requirements 7
3.2. Transfer Encoding Definition Procedure 7
3.3. IANA Procedures for Transfer Encoding Registration 8
3.4. Location of Registered Transfer Encodings List 8
4. Security Considerations 8
5. IANA Considerations 8
6. Acknowledgements 8
7. References 9
A. Changes Since RFC 2048 9

1. Introduction

Recent Internet protocols have been carefully designed to be easily extensible in certain areas. In particular, MIME [RFC2045] is an open-ended framework and can accommodate additional object types, charsets, and access methods without any changes to the basic protocol. A registration process is needed, however, to ensure that the set of such values is developed in an orderly, well-specified, and public manner.

This document defines registration procedures that use the Internet Assigned Numbers Authority (IANA) as a central registry for these values.

Note:

Registration of media types and charsets for use in MIME are specified in separate documents [RFC4288] [RFC2978] and are not addressed here.

1.1. 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. External Body Access Types

[RFC2046] defines the message/external-body media type, whereby a MIME entity can act as pointer to the actual body data in lieu of including the data directly in the entity body. Each message/external-body reference specifies an access type, which determines the mechanism used to retrieve the actual body data. RFC 2046 defines an initial set of access types but allows for the registration of additional access types to accommodate new retrieval mechanisms.

2.1. Registration Requirements

New access type specifications MUST conform to the requirements described below.

2.1.1. Naming Requirements

Each access type MUST have a unique name. This name appears in the access-type parameter in the message/external-body content-type header field and MUST conform to MIME content type parameter syntax.

2.1.2. Mechanism Specification Requirements

All of the protocols, transports, and procedures used by a given access type MUST be described, either in the specification of the access type itself or in some other publicly available specification, in sufficient detail for the access type to be implemented by any competent implementor. Use of secret and/or proprietary methods in access types is expressly prohibited. The restrictions imposed by [RFC2026] on the standardization of patented algorithms must be respected as well.

2.1.3. Publication Requirements

All access types MUST be described by an RFC. The RFC may be informational rather than standards-track, although standards-track review and approval are encouraged for all access types.

2.1.4. Security Requirements

Any known security issues that arise from the use of the access type MUST be completely and fully described. It is not required that the access type be secure or that it be free from risks, but it is required that the known risks be identified. Publication of a new access type does not require an exhaustive security review, and the security considerations section is subject to continuing evaluation. Additional security considerations SHOULD be addressed by publishing revised versions of the access type specification.

2.2. Registration Procedure

Registration of a new access type starts with the publication of the specification as an Internet Draft.

2.2.1. Present the Access Type to the Community

A proposed access type specification is sent to the "ietf-types@iana.org" mailing list for a two-week review period. This mailing list has been established for the purpose of reviewing proposed access and media types. Proposed access types are not formally registered and must not be used.

The intent of the public posting is to solicit comments and feedback on the access type specification and a review of any security considerations.

2.2.2. Access Type Reviewer

When the two-week period has passed, the access type reviewer, who is appointed by the IETF Applications Area Director(s), either forwards the request to iana@iana.org or rejects it because of significant objections raised on the list.

Decisions made by the reviewer must be posted to the ietf-types mailing list within 14 days. Decisions made by the reviewer may be appealed to the IESG as specified in [RFC2026].

2.2.3. IANA Registration

Provided that the access type either has passed review or has been successfully appealed to the IESG, the IANA will register the access type and make the registration available to the community. The specification of the access type must also be published as an RFC.

2.3. Location of Registered Access Type List

Access type registrations are listed by the IANA on the following web page:

http://www.iana.org/assignments/access-types

2.4. IANA Procedures for Registering Access Types

The identity of the access type reviewer is communicated to the IANA by the IESG. The IANA then only acts either in response to access type definitions that are approved by the access type reviewer and forwarded to the IANA for registration, or in response to a communication from the IESG that an access type definition appeal has overturned the access type reviewer's ruling.

3. Transfer Encodings

Transfer encodings are transformations applied to MIME media types after conversion to the media type's canonical form. Transfer encodings are used for several purposes:

- Many transports, especially message transports, can only handle data consisting of relatively short lines of text. There can be severe restrictions on what characters can be used in these lines of text. Some transports are restricted to a small subset of US-ASCII, and others cannot handle certain character sequences. Transfer encodings are used to transform binary data into a textual form that can survive such transports. Examples of this sort of transfer encoding include the base64 and quoted-printable transfer encodings defined in [RFC2045].

- Image, audio, video, and even application entities are sometimes quite large. Compression algorithms are often effective in reducing the size of large entities. Transfer encodings can be used to apply general-purpose non-lossy compression algorithms to MIME entities.

- Transport encodings can be defined as a means of representing existing encoding formats in a MIME context.

IMPORTANT: The standardization of a large number of different transfer encodings is seen as a significant barrier to widespread interoperability and is expressly discouraged. Nevertheless, the following procedure has been defined in order to provide a means of defining additional transfer encodings, should standardization actually be justified.

3.1. Transfer Encoding Requirements

Transfer encoding specifications MUST conform to the requirements described below.

3.1.1. Naming Requirements

Each transfer encoding MUST have a unique name. This name appears in the Content-Transfer-Encoding header field and MUST conform to the syntax of that field.

3.1.2. Algorithm Specification Requirements

All of the algorithms used in a transfer encoding (e.g., conversion to printable form, compression) MUST be described in their entirety in the transfer encoding specification. Use of secret and/or

proprietary algorithms in standardized transfer encodings is expressly prohibited. The restrictions imposed by [RFC2026] on the standardization of patented algorithms MUST be respected as well.

3.1.3. Input Domain Requirements

All transfer encodings MUST be applicable to an arbitrary sequence of octets of any length. Dependence on particular input forms is not allowed.

It should be noted that the 7bit and 8bit encodings do not conform to this requirement. Aside from the undesirability of having specialized encodings, the intent here is to forbid the addition of additional encodings similar to, or redundant with, 7bit and 8bit.

3.1.4. Output Range Requirements

There is no requirement that a particular transfer encoding produce a particular form of encoded output. However, the output format for each transfer encoding MUST be fully and completely documented. In particular, each specification MUST clearly state whether the output format always lies within the confines of 7bit or 8bit or is simply pure binary data.

3.1.5. Data Integrity and Generality Requirements

All transfer encodings MUST be fully invertible on any platform; it MUST be possible for anyone to recover the original data by performing the corresponding decoding operation. Note that this requirement effectively excludes all forms of lossy compression as well as all forms of encryption from use as a transfer encoding.

3.1.6. New Functionality Requirements

All transfer encodings MUST provide some sort of new functionality. Some degree of functionality overlap with previously defined transfer encodings is acceptable, but any new transfer encoding MUST also offer something no other transfer encoding provides.

3.1.7. Security Requirements

To the greatest extent possible, transfer encodings SHOULD NOT contain known security issues. Regardless, any known security issues that arise from the use of the transfer encoding MUST be completely and fully described. If additional security issues come to light after initial publication and registration, they SHOULD be addressed by publishing revised versions of the transfer encoding specification.

3.2. Transfer Encoding Definition Procedure

Definition of a new transfer encoding starts with the publication of the specification as an Internet Draft. The draft MUST define the transfer encoding precisely and completely, and it MUST also provide substantial justification for defining and standardizing a new transfer encoding. This specification MUST then be presented to the IESG for consideration. The IESG can:

- reject the specification outright as being inappropriate for standardization,
- assign the specification to an existing IETF working group for further work,
- approve the formation of an IETF working group to work on the specification in accordance with IETF procedures, or
- accept the specification as-is for processing as an individual standards-track submission.

Transfer encoding specifications on the standards track follow normal IETF rules for standards-track documents. A transfer encoding is

considered to be defined and available for use once it is on the standards track.

3.3. IANA Procedures for Transfer Encoding Registration

There is no need for a special procedure for registering Transfer Encodings with the IANA. All legitimate transfer encoding registrations MUST appear as a standards-track RFC, so it is the IESG's responsibility to notify the IANA when a new transfer encoding has been approved.

3.4. Location of Registered Transfer Encodings List

The list of transfer encoding registrations can be found at:

http://www.iana.org/assignments/transfer-encodings

4. Security Considerations

Security requirements for access types are discussed in Section 2.1.4. Security requirements for transfer encodings are discussed in Section 3.1.7.

5. IANA Considerations

The sole purpose of this document is to define IANA registries for access types and transfer encodings. The IANA procedures for these registries are specified in Section 2.4 and Section 3.3 respectively.

6. Acknowledgements

The current authors would like to acknowledge their debt to the late Dr. Jon Postel, whose general model of IANA registration procedures and specific contributions shaped the predecessors of this document [RFC2048]. We hope that the current version is one with which he would have agreed but, as it is impossible to verify that agreement, we have regretfully removed his name as a co-author.

7. References

7.1. Normative References

[RFC2045] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996.

[RFC2046] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", RFC 2046, November 1996.

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

[RFC4288] Freed, N. and J. Klensin, "Media Type Specifications and Registration Procedures", BCP 13, RFC 4288, December 2005.

7.2. Informative References

[RFC2026] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

[RFC2048] Freed, N., Klensin, J., and J. Postel, "Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures", BCP 13, RFC 2048, November 1996.

[RFC2978] Freed, N. and J. Postel, "IANA Charset Registration Procedures", BCP 19, RFC 2978, October 2000.

Appendix A. Changes Since RFC 2048

- Media type registration procedures are now described in a separate document [RFC4288].
- The various URLs and addresses in this document have been changed so they all refer to iana.org rather than isi.edu. Additionally, many of the URLs have been changed to use HTTP; formerly they used FTP.
- Much of the document has been clarified in the light of operational experience with these procedures.
- Several of the references in this document have been updated to refer to current versions of the relevant specifications.
- The option of assigning the task of working on a new transfer encoding to an existing working group has been added to the list of possible actions the IESG can take.
- Security considerations and IANA considerations sections have been added.
- Registration of charsets for use in MIME is specified in [RFC2978] and is no longer addressed by this document.

Authors' Addresses

Ned Freed
Sun Microsystems
3401 Centrelake Drive, Suite 410
Ontario, CA 92761-1205
USA

Phone: +1 909 457 4293
EMail: ned.freed@mrochek.com

John C. Klensin
1770 Massachusetts Ave, #322
Cambridge, MA 02140

EMail: klensin+ietf@jck.com

Full Copyright Statement

Copyright (C) The Internet Society (2005).

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.

Intellectual Property

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.

Acknowledgement

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