Internet Draft: Message Submission for Mail
Document: draft-gellens-submit-bis-02.txt
Expires: September 2005
Obsoletes: RFC 2476

R. Gellens
QUALCOMM
J. Klensin

March 2005

Message Submission for Mail

Status of this Memo

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed and any of which I become aware will be disclosed, in accordance with RFC 3668 (BCP 79).

By submitting this Internet-Draft, I accept the provisions of Section 3 of RFC 3667 (BCP 78).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Comments:

Public comments should be sent to the IETF Submit mailing list, <ietf-submit@imc.org>. To subscribe, send a message containing SUBSCRIBE to <ietf-submit-request@imc.org>. This list will remain active after publication. Private comments may be sent to the authors.

Copyright Notice

Abstract

This memo splits message submission from message relay, allowing each service to operate according to its own rules (for security, policy, etc.), and specifies what actions are to be taken by a submission server.

Message relay is unaffected, and continues to use SMTP [SMTP-MTA] over port 25.

When conforming to this document, message submission uses the protocol specified here, normally over port 587.

This separation of function offers a number of benefits, including the ability to apply specific security or policy requirements.

Table of Contents

1. Introduction 3
2. Document Information 5
2.1. Definitions of Terms Used in this Memo 5
2.2. Conventions Used in this Document 5
3. Message Submission 6
3.1. Submission Identification 6
3.2. Message Rejection and Bouncing 6
3.3. Authorized Submission 7
4. Mandatory Actions 8
4.1. General Submission Rejection Code 8
4.2. Ensure All Domains are Fully-Qualified 8
4.3. Require Authentication 8
5. Recommended Actions 9
5.1. Enforce Address Syntax 9
5.2. Log Errors 9
6. Optional Actions 9
6.1. Enforce Submission Rights 9
6.2. Enforce Permissions 10
6.3. Check Message Data 10
6.4 Support for the Postmaster Address 10
7. Interaction with SMTP Extensions 10
8. Message Modifications 12
8.1. Add 'Sender' 12
8.2. Add 'Date' 12
8.3. Add 'Message-ID' 12
8.4. Transfer Encode 12
8.5. Sign the Message 13
8.6. Encrypt the Message 13
8.7. Resolve Aliases 13
8.8. Header Rewriting 13
9. Security Considerations 14
10. IANA Considerations 14
11. Acknowledgments 14
12. Normative References 15
13. Informative References 15
14. Authors' Addresses 17
Appendix A: Changes from RFC 2476 17
Intellectual Property Statement 17
Full Copyright Statement 18
Disclaimer 18

1. Introduction

SMTP was defined as a message *transfer* protocol, that is, a means to route (if needed) and deliver finished (complete) messages.

Message Transfer Agents (MTAs) are not supposed to alter the message text, except to add 'Received', 'Return-Path', and other header fields as required by [SMTP-MTA].

However, SMTP is now also widely used as a message *submission* protocol, that is, a means for message user agents (MUAs) to introduce new messages into the MTA routing network. The process which accepts message submissions from MUAs is termed a Message Submission Agent (MSA).

In order to permit unconstrained communications, SMTP is not often authenticated during message relay.

Authentication and authorization of initial submissions has become increasingly important, driven by changes in security requirements and rising expectations that submission servers take responsibility for the message traffic they originate. For example, many sites now prohibit outbound port 25 traffic, funneling all mail submissions through submission servers, due to the prevalence of machines that have worms, viruses, or other malicious software which generate large amounts of spam.

In addition to authentication and authorization issues, messages being submitted are in some cases finished (complete) messages, and in other cases are unfinished (incomplete) in one or more aspects. Unfinished messages may need to be completed to ensure they conform to [MESSAGE-FORMAT], and later requirements. For example, the message may lack a proper 'Date' header field, and domains might not be fully qualified. In some cases, the MUA may be unable to generate finished messages (for example, it might not know its time zone). Even when submitted messages are complete, local site policy may dictate that the message text be examined or modified in some way. Such completions or modifications have been shown to cause harm when performed by downstream MTAs -- that is, MTAs after the first-hop submission MTA -- and are in general considered to be outside the province of standardized MTA functionality.

Separating messages into submissions and transfers allows developers and network administrators to more easily:

* Implement security policies and guard against unauthorized mail relaying or injection of unsolicited bulk mail

* Implement authenticated submission, including off-site submission by authorized users such as travelers

* Separate the relevant software code differences, thereby making each code base more straightforward and allowing for different programs for relay and submission

* Detect configuration problems with a site's mail clients

* Provide a basis for adding enhanced submission services in the future

This memo describes a low cost, deterministic means for messages to be identified as submissions, and specifies what actions are to be taken by a submission server.

2. Document Information

2.1. Definitions of Terms Used in this Memo

Fully-Qualified

Containing or consisting of a domain which can be globally resolved using the global Domain Name Service; that is, not a local alias or partial specification.

Message Submission Agent (MSA)

A process which conforms to this specification. An MSA acts as a submission server to accept messages from MUAs, and either delivers them or acts as an SMTP client to relay them to an MTA.

Message Transfer Agent (MTA)

A process which conforms to [SMTP-MTA]. An MTA acts as an SMTP server to accept messages from an MSA or another MTA, and either delivers them or acts as an SMTP client to relay them to another MTA.

Message User Agent (MUA)

A process which acts (often on behalf of a user and with a user interface) to compose and submit new messages, and process delivered messages. In what is commonly referred to as a split-MUA model, POP [POP3] or IMAP [IMAP4] is used to access delivered messages while the protocol defined here (or SMTP) is used to submit messages.

2.2. Conventions Used in this Document

In examples, "C:" is used to indicate lines sent by the client, and "S:" indicates those sent by the server. Line breaks within a command example are for editorial purposes only.

Examples use the 'example.net' domain.

The key words "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", and "MAY" in this document are to be interpreted as defined in [KEYWORDS].

3. Message Submission

3.1. Submission Identification

Port 587 is reserved for email message submission as specified in this document. Messages received on this port are defined to be submissions. The protocol used is ESMTP [SMTP-MTA, ESMTP], with additional restrictions or allowances as specified here.

While most email clients and servers can be configured to use port 587 instead of 25, there are cases where this is not possible or convenient. A site MAY choose to use port 25 for message submission, by designating some hosts to be MSAs and others to be MTAs.

3.2. Message Rejection and Bouncing

MTAs and MSAs MAY implement message rejection rules that rely in part on whether the message is a submission or a relay.

For example, some sites might configure their MTAs to reject all RCPT TOs for messages that do not reference local users, and configure their MSA to reject all message submissions that do not come from authorized users, with authorization based either on the submitting endpoint being within a protected IP environment, or authenticated identity.

NOTE: It is better to reject a message than to risk sending one that is damaged. This is especially true for problems that are correctable by the MUA, for example, an invalid 'From' field.

If an MSA is not able to determine a return path to the submitting user, from a valid MAIL FROM, a valid source IP address, or based on authenticated identity, then the MSA SHOULD immediately reject the message. A message can be immediately rejected by returning a 550 code to the MAIL FROM command.

Note that a null return path, that is, MAIL FROM:<>, is permitted and MUST NOT in itself be cause for rejecting a message. (MUAs need to generate null return-path messages for a variety of reasons, including disposition notifications.)

Except in the case where the MSA is unable to determine a valid return path for the message being submitted, text in this specification which instructs an MSA to issue a rejection code MAY be complied with by accepting the message and subsequently generating a bounce message. (That is, if the MSA is going to reject a message for any reason except being unable to determine a return path, it can optionally do an immediate rejection or accept the message and then mail a bounce.)

NOTE: In the normal case of message submission, immediately rejecting the message is preferred, as it gives the user and MUA direct feedback. To properly handle delayed bounces the client MUA needs to maintain a queue of messages it has submitted, and match bounces to them. Note that many contemporary MUAs do not have this capability.

3.3. Authorized Submission

Numerous methods have been used to ensure that only authorized users are able to submit messages. These methods include authenticated SMTP, IP address restrictions, secure IP, and prior POP authentication.

Authenticated SMTP [SMTP-AUTH] has seen widespread deployment. It allows the MSA to determine an authorization identity for the message submission, which is not tied to other protocols.

IP address restrictions are very widely implemented, but do not allow for travelers and similar situations, and can be easily spoofed unless all transport paths between the MUA and MSA are trustworthy.

Secure IP [IPSEC] can also be used, and provides additional benefits of protection against eavesdropping and traffic analysis.

Requiring a POP [POP3] authentication (from the same IP address) within some amount of time (for example, 20 minutes) prior to the start of a message submission session has also been used, but this does impose restrictions on clients as well as servers which may cause difficulties. Specifically, the client must do a POP authentication before an SMTP submission session, and not all clients are capable and configured for this. Also, the MSA must coordinate with the POP server, which may be difficult. There is

also a window during which an unauthorized user can submit messages and appear to be a previously authorized user. Since it is dependent on the MUA's IP addresses, this technique is substantially as subject to IP address spoofing as validation based on known IP addresses alone (see above).

4. Mandatory Actions

An MSA MUST do all of the following:

4.1. General Submission Rejection Code

Unless covered by a more precise response code, response code 554 is to be used to reject a MAIL FROM, RCPT TO, or DATA command that contains something improper.

4.2. Ensure All Domains are Fully-Qualified

The MSA MUST ensure that all domains in the SMTP envelope are fully-qualified.

If the MSA examines or alters the message text in any way, except to add trace header fields [SMTP-MTA], it MUST ensure that all domains in address header fields are fully-qualified.

Reply code 554 is to be used to reject a MAIL FROM, RCPT TO, or DATA command which contains improper domain references.

A frequent local convention is to accept single-level domains (for example, 'sales') and then to expand the reference by adding the remaining portion of the domain name (for example, to 'sales.example.net'). Local conventions that permit single-level domains SHOULD reject, rather than expand, incomplete multi-level domains, since such expansion is particularly risky.

4.3. Require Authentication

The MSA MUST by default issue an error response to the MAIL FROM command if the session has not been authenticated using [SMTP-AUTH], unless it has already independently established authentication or authorization (such as being within a protected subnetwork).

Section 3.3 discusses authentication mechanisms.

Reply code 530 [SMTP-AUTH] is used for this purpose.

5. Recommended Actions

The MSA SHOULD do all of the following:

5.1. Enforce Address Syntax

An MSA SHOULD reject messages with illegal syntax in a sender or recipient SMTP envelope address.

If the MSA examines or alters the message text in way, except to add trace header fields, it SHOULD reject messages with illegal address syntax in address header fields.

Reply code 501 is to be used to reject a MAIL FROM or RCPT TO command that contains a detectably improper address.

When addresses are resolved after submission of the message body, reply code 554 (with a suitable enhanced status code from [SMTP-CODES]) is used after end-of-data, if the message contains invalid addresses in the header.

5.2. Log Errors

The MSA SHOULD log message errors, especially apparent misconfigurations of client software.

It can be very helpful to notify the administrator when problems are detected with local mail clients. This is another advantage of distinguishing submission from relay: system administrators might be interested in local configuration problems, but not in client problems at other sites.

Note that it is important to impose limits on such logging to prevent certain forms of DOS attacks.

6. Optional Actions

The MSA MAY do any of the following:

6.1. Enforce Submission Rights

The MSA MAY issue an error response to the MAIL FROM command if the address in MAIL FROM appears to have insufficient submission rights, or is not authorized with the authentication used (if the session has been authenticated).

Reply code 550 with an appropriate enhanced status code per [SMTP-CODES], such as 5.7.1, is used for this purpose.

6.2. Enforce Permissions

The MSA MAY issue an error response to the RCPT TO command if inconsistent with the permissions given to the user (if the session has been authenticated).

Reply code 550 with an appropriate enhanced status code per [SMTP-CODES], such as 5.7.1, is used for this purpose.

6.3. Check Message Data

The MSA MAY issue an error response to the DATA command or send a failure result after end-of-data if the submitted message is syntactically invalid, or seems inconsistent with permissions given to the user (if known), or violates site policy in some way.

Reply code 554 is used for syntactic problems in the data. Reply code 501 is used if the command itself is not syntactically valid. Reply code 550 with an appropriate enhanced status code per [SMTP-CODES] (such as 5.7.1) is used to reject based on the submitting user. Reply code 550 with an appropriate enhanced status code (such as 5.7.0) is used if the message violates site policy.

6.4 Support for the Postmaster Address

If appropriate under local conditions and to facilitate conformance with the "postmaster" requirements of [SMTP-MTA], the MSA MAY permit a reduced degree of authentication for mail addressed to the "postmaster" (or one of its alternate spelling forms, see [SMTP-MTA]), in one or more domains, as compared to requirements enforced for other addresses. Among other benefits, this provides an address of last resort that can be used by authorized users to report problems that otherwise prevent them from submitting mail.

7. Interaction with SMTP Extensions

The following table lists the current standards-track and Experimental SMTP extensions. Listed are the EHLO keyword, name, an indication as to the use of the extension on the submit port, and a reference:

Keyword	Name	Submission	Reference
PIPELINING	Pipelining	SHOULD	[PIPELINING]
ENHANCEDSTATUSCODES	Enhanced Status Codes	SHOULD	[CODES-EXTENSION]
ETRN	Extended Turn	MUST NOT	[ETRN]
...	Extended Codes	SHOULD	[SMTP-CODES]
DSN	Delivery Status Notification	SHOULD	[DSN]
SIZE	Message size	MAY	[SIZE]
...	521 reply code	MUST NOT	[521REPLY]
CHECKPOINT	Checkpoint/Restart	MAY	[Checkpoint]
BINARYMIME	Binary MIME	MAY	[CHUNKING]
CHUNKING	Chunking	MAY	[CHUNKING]
8BITMIME	Use 8-bit data	SHOULD	[8BITMIME]
AUTH	Authentication	MUST	[SMTP-AUTH]
STARTTLS	Start TLS	MAY	[Start-TLS]
NO-SOLICITING	Notification of no soliciting	MAY	[Msg-Track]
MTRK	Message Tracking	MAY	[Msg-Track]

Future SMTP extensions SHOULD explicitly specify if they are valid on the Submission port.

Some SMTP extensions are especially useful for message submission:

Extended Status Codes [SMTP-CODES] SHOULD be supported and used according to [CODES-EXTENSION]. This permits the MSA to notify the client of specific configuration or other problems in more detail than the response codes listed in this memo. Because some rejections are related to a site's security policy, care should be used not to expose more detail than is needed to correct the problem.

[PIPELINING] SHOULD be supported by the MSA.

[SMTP-AUTH] allows the MSA to validate the authority and determine the identity of the submitting user and MUST be supported by the MSA.

Any references to the DATA command in this memo also refer to any substitutes for DATA, such as the BDAT command used with [CHUNKING].

8. Message Modifications

Sites MAY modify submissions to ensure compliance with standards and site policy. This section describes a number of such modifications that are often considered useful.

NOTE: As a matter of guidance for local decisions to implement message modification, a paramount rule is to limit such actions to remedies for specific problems that have clear solutions. This is especially true with address elements. For example, indiscriminately appending a domain to an address or element which lacks one typically results in more broken addresses. An unqualified address must be verified to be a valid local part in the domain before the domain can be safely added.

8.1. Add 'Sender'

The MSA MAY add or replace the 'Sender' field, if the identity of the sender is known and this is not given in the 'From' field.

The MSA MUST ensure that any address it places in a 'Sender' field is in fact a valid mail address.

8.2. Add 'Date'

The MSA MAY add a 'Date' field to the submitted message, if it lacks it, or correct the 'Date' field if it does not conform to [MESSAGE-FORMAT] syntax.

8.3. Add 'Message-ID'

The MSA SHOULD add or replace the 'Message-ID' field, if it lacks it, or it is not valid syntax (as defined by [MESSAGE-FORMAT]). Note that a number of clients still do not generate Message-Id fields.

8.4. Transfer Encode

The MSA MAY apply transfer encoding to the message according to MIME conventions, if needed and not harmful to the MIME type.

8.5. Sign the Message

The MSA MAY (digitally) sign or otherwise add authentication information to the message.

8.6. Encrypt the Message

The MSA MAY encrypt the message for transport to reflect organizational policies.

NOTE: To be useful, the addition of a signature and/or encryption by the MSA generally implies that the connection between the MUA and MSA must itself be secured in some other way, e.g., by operating inside of a secure environment, by securing the submission connection at the transport layer, or by using an [SMTP-AUTH] mechanism that provides for session integrity.

8.7. Resolve Aliases

The MSA MAY resolve aliases (CNAME records) for domain names, in the SMTP envelope and optionally in address fields of the header, subject to local policy.

NOTE: Unconditionally resolving aliases could be harmful. For example, if www.example.net and ftp.example.net are both aliases for mail.example.net, rewriting them could lose useful information.

8.8. Header Rewriting

The MSA MAY rewrite local parts and/or domains in the SMTP envelope, and optionally in address fields of the header, according to local policy. For example, a site may prefer to rewrite 'JRU' as 'J.Random.User' in order to hide login names, and/or to rewrite 'squeaky.sales.example.net' as 'zyx.example.net' to hide machine names and make it easier to move users.

However, only addresses, local-parts, or domains which match specific local MSA configuration settings should be altered. It would be very dangerous for the MSA to apply data-independent rewriting rules, such as always deleting the first element of a domain name. So, for example, a rule which strips the left-most element of the domain if the complete domain matches

'*.foo.example.net' would be acceptable.

9. Security Considerations

Separation of submission and relay of messages can allow a site to implement different policies for the two types of services, including requiring use of additional security mechanisms for one or both. It can do this in a way which is simpler, both technically and administratively. This increases the likelihood that policies will be applied correctly.

Separation also can aid in tracking and preventing unsolicited bulk email.

For example, a site could configure its mail servers such that the MSA requires authentication before accepting a message, and the MTA rejects all RCPT TOs for non-local users. This can be an important element in a site's total email security policy.

If a site fails to require any form of authorization for message submissions (see section 3.3 for discussion), it is allowing open use of its resources and name; unsolicited bulk email can be injected using its facilities.

Section 3 includes further discussion of issues with some authentication methods.

Section 5.2 includes a cautionary note that unlimited logging can enable certain forms of denial of service attacks.

10. IANA Considerations

The registration for port 587 should be updated to refer to this memo rather than RFC 2476.

11. Acknowledgments

Nathaniel Borenstein and Barry Leiba were instrumental in the development of this update to RFC 2476.

The original memo (RFC 2476) was developed in part based on comments and discussions which took place on and off the IETF-Submit mailing list. The help of those who took the time to review that draft and make suggestions is appreciated, especially that of Dave Crocker, Ned Freed, Keith Moore, John Myers, and Chris Newman.

Special thanks to Harald Alvestrand, who got this effort started.

12. Normative References

[ABNF] D. Crocker, Ed., P. Overell, "Augmented BNF for Syntax Specifications: ABNF", November 1997, RFC 2234, <ftp://ftp.isi.edu/in-notes/rfc2234.txt>

[ESMTP] J. Klensin, N. Freed, M. Rose, E. Stefferud, and D. Crocker, "SMTP Service Extensions", November 1995, STD 10, RFC 1869, <ftp://ftp.isi.edu/in-notes/rfc1869.txt>

[KEYWORDS] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", March 1997, BCP 14, RFC 2119, <ftp://ftp.isi.edu/in-notes/rfc2119.txt>

[SMTP-MTA] J. Postel, "Simple Mail Transfer Protocol", August 1982, STD 10, RFC 821, <ftp://ds.internic.net/rfc/rfc821.txt>; C. Partridge, "Mail Routing and the Domain System", January 1986, STD 14, RFC 974, <ftp://ds.internic.net/rfc/rfc974.txt>; R. Braden, Editor, "Requirements for Internet Hosts -- Application and Support", October 1989, STD 3, RFC 1123, <ftp://ftp.isi.edu/in-notes/rfc1123.txt>; note that an updated document which unifies and clarifies material has been published as: J. Klensin, "Simple Mail Transfer Protocol", April 2001, RFC 2821, <ftp://ftp.isi.edu/in-notes/rfc2821.txt>

13. Informative References

[521REPLY] A. Durand, and F. Dupont, "SMTP 521 Reply Code", September 1995, <ftp://ftp.isi.edu/in-notes/rfc1846.txt>

[8BITMIME] J. Klensin, N. Freed, M. Rose, E. Stefferud, and D. Crocker, "SMTP Service Extension for 8bit-MIMEtransport", July 1994, <ftp://ftp.isi.edu/in-notes/rfc1652.txt>

[CHECKPOINT] D. Crocker, N. Freed, and A. Cargille, "SMTP Service Extension for Checkpoint/Restart, September 1995, RFC 1845, <ftp://ftp.isi.edu/in-notes/rfc1845.txt>

[CHUNKING] G. Vaudreuil, "SMTP Service Extensions for Transmission of Large and Binary MIME Messages", December 2000, RFC 3030, <ftp://ftp.isi.edu/in-notes/rfc3030.txt>

[CODES-EXTENSION] N. Freed, "SMTP Service Extension for Returning Enhanced Error Codes", October 1996, RFC 2034, <ftp://ftp.isi.edu/in-notes/rfc2034.txt>

[DSN] K. Moore, "Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)", January 2003, RFC 3461, <ftp://ftp.isi.edu/in-notes/rfc3461.txt>

[ETRN] J. De Winter, "SMTP Service Extension for Remote Message Queue Starting", August 1996, RFC 1985, <ftp://ftp.isi.edu/in-notes/rfc1985.txt>

[HEADERS] J. Palme, "Common Internet Message Headers", February 1997, RFC 2076, <ftp://ftp.isi.edu/in-notes/rfc2076.txt>

[IMAP4] M. Crispin, "INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1", March 2003, RFC 3501, <ftp://ftp.isi.edu/in-notes/rfc3501.txt>

[IPSEC] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol", November 1998, RFC 2401, <ftp://ftp.isi.edu/in-notes/rfc2401.txt>

[MESSAGE-FORMAT] D. Crocker, "Standard for the format of ARPA Internet text messages", August 1982, STD 11, RFC 822, <ftp://ds.internic.net/rfc/rfc822.txt>; R. Braden, Editor, "Requirements for Internet Hosts -- Application and Support", October 1989, STD 3, RFC 1123, <ftp://ftp.isi.edu/in-notes/rfc1123.txt>

[Msg-Track] E. Allman, T. Hansen, "SMTP Service Extension for Message Tracking", September 2004, RFC 3885, <ftp://ftp.isi.edu/in-notes/rfc3885.txt>

[PIPELINING] N. Freed, "SMTP Service Extension for Command Pipelining", September 2000, RFC 2920, STD 60, <ftp://ftp.isi.edu/in-notes/rfc2920.txt>

[POP3] J. Myers, M. Rose, "Post Office Protocol -- Version 3", STD 53, May 1996, RFC 1939, <ftp://ftp.isi.edu/in-notes/rfc1939.txt>

[SIZE] J. Klensin, N. Freed, and K. Moore, "SMTP Service Extension for Message Size Declaration, November 1995, RFC 1870, STD 10, <ftp://ftp.isi.edu/in-notes/rfc1870.txt>

[SMTP-AUTH] J. Myers, "SMTP Service Extension for Authentication", March 1999, RFC 2554, <ftp://ftp.isi.edu/in-notes/rfc2554.txt>

[SMTP-CODES] G. Vaudreuil, "Enhanced Mail System Status Codes", January 2003, RFC 3463, <ftp://ftp.isi.edu/in-notes/rfc3463.txt>

[Start-TLS] P. Hoffman, "SMTP Service Extension for Secure SMTP over Transport Layer Security", February 2002, RFC 3207, <ftp://ftp.isi.edu/in-notes/rfc3207.txt>

14. Authors' Addresses

Randall Gellens
QUALCOMM Incorporated
6455 Lusk Blvd.
San Diego, CA 92121-2779
USA
randy@qualcomm.Com

John C. Klensin
1770 Massachusetts Ave, #322
Cambridge, MA 02140
USA
john+ietf@jck.com

Appendix A: Changes from RFC 2476

- Support for [SMTP-AUTH] is now mandatory
- Message-ID changed from MAY to SHOULD
- Added NO-SOLICITING and MTRK (RFC 3885) to list of SMTP extensions
- Deleted normative use of specific enhanced status codes, to avoid conflicting with [SMTP-CODES]
- Section 4.2 text no longer in a note
- Fixed a few typographical errors

Intellectual Property Statement

proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement

Disclaimer