Network Working Group
Request for Comments: 2476
Category: Standards Track
December 1998

R. Gellens
QUALCOMM
J. Klensin
MCI

Message Submission

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Table of Contents

1. Abstract

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).

Messages being submitted are in some cases finished (complete) messages, and in other cases are unfinished (incomplete) in some aspect or other. Unfinished messages 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.

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>. Private comments may be sent to the authors.

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, which 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], which 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 (usually on behalf of a user) to compose and submit new messages, and process delivered messages. In the split-MUA model, POP or IMAP is used to access delivered 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 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 MTA 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, based on IP address, 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 be accepted. (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 must maintain a queue of messages it has submitted, and match bounces to them.

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 been proposed. 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 travellers and similar situations, and can be spoofed.

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 prior authorized user.

3.4. Enhanced Status Codes

This memo suggests several enhanced status codes [SMTP-CODES] for submission-specific rejections. The specific codes used are:

5.6.0 Bad content. The content of the header or text is improper.

5.6.2 Bad domain or address. Invalid or improper domain or address in MAIL FROM, RCPT TO, or DATA.

5.7.1 Not allowed. The address in MAIL FROM appears to have insufficient submission rights, or is invalid, or is not authorized with the authentication used; the address in a RCPT TO command is inconsistent with the permissions given to the user; the message data is rejected based on the submitting user.

5.7.0 Site policy. The message appears to violate site policy in some way.

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. Enhanced status code 5.6.0 is to be used if no other code is more specific.

4.2. Ensure All Domains are Fully-Qualified

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

If the MSA examines or alters the message text in 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.

NOTE: 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.

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 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 enhanced status code 5.6.2 is to be 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.

Note: 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.

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 enhanced status code 5.7.1 is used for this purpose.

6.2. Require Authentication

The MSA MAY issue an error response to the MAIL FROM command if the session has not been authenticated.

Section 3.3 discusses authentication mechanisms.

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

6.3. 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 enhanced status code 5.7.1 is used for this purpose.

6.4. 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 enhanced status code 5.7.1 is used to reject based on the submitting user. Reply code 550 with enhanced status code 5.7.0 is used if the message violates site policy.

7. Interaction with SMTP Extensions

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

RFC	Name	Submission	Reference
2197	Pipelining	SHOULD	[PIPELINING]
2034	Error Codes	SHOULD	[CODES-EXTENSION]
1985	ETRN	MUST NOT	[ETRN]
1893	Extended Codes	SHOULD	[SMTP-CODES]
1891	DSN	SHOULD	[DSN]
1870	Size	MAY	[SIZE]
1846	521	MUST NOT	[521REPLY]
1845	Checkpoint	MAY	[Checkpoint]

1830	Binary	MAY	[CHUNKING]
1652	8-bit MIME	SHOULD	[8BITMIME]
----	Authentication	------	[SMTP-AUTH]

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.

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 MAY add or replace the ’Message-ID’ field, if it lacks it, or it is not valid syntax (as defined by [MESSAGE-FORMAT]).

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 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 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 logon names, and/or to rewrite ’ squeeky.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 MSA to require authentication before accepting a message, and could configure its MTA to reject 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.

10. Acknowledgments

This updated memo has been revised 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 the 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.

11. References

[521REPLY] Durand, A. and F. Dupont, "SMTP 521 Reply Code", RFC 1846, September 1995.

[8BITMIME] Klensin, J., Freed, N., Rose, M., Stefferud, E. and D. Crocker, "SMTP Service Extension for 8bit-MIMEtransport", RFC 1652, July 1994.

[ABNF] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, November 1997.

[CHECKPOINT] Crocker, D., Freed, N. and A. Cargille, "SMTP Service Extension for Checkpoint/Restart", RFC 1845, September 1995.

[CHUNKING] Vaudreuil, G., "SMTP Service Extensions for Transmission of Large and Binary MIME Messages", RFC 1830, August 1995.

[CODES-EXTENSION] Freed, N., "SMTP Service Extension for Returning Enhanced Error Codes", RFC 2034, October 1996.

[DSN] Moore, K., "SMTP Service Extension for Delivery Status Notifications", RFC 1891, January 1996.

[ESMTP] Klensin, J., Freed, N., Rose, M., Stefferud, E. and D. Crocker, "SMTP Service Extensions", STD 10, RFC 1869, November 1995.

[ETRN] De Winter, J., "SMTP Service Extension for Remote Message Queue Starting", RFC 1985, August 1996.

[HEADERS] Palme, J., "Common Internet Message Headers", RFC 2076, February 1997.

[IPSEC] Atkinson, R., "Security Architecture for the Internet Protocol", RFC 1825, August 1995.

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

[MESSAGE-FORMAT] Crocker, D., "Standard for the format of ARPA Internet text messages", STD 11, RFC 822, August 1982;

Braden, R., Editor, "Requirements for Internet Hosts -- Application and Support", STD 3, RFC 1123, October 1989.

[PIPELINING] Freed, N., "SMTP Service Extension for Command Pipelining", RFC 2197, September 1997.

[POP3] Myers, J. and M. Rose, "Post Office Protocol -- Version 3", STD 53, RFC 1939, May 1996.

[SIZE] Klensin, J., Freed, N. and K. Moore, "SMTP Service Extension for Message Size Declaration", STD 10, RFC 1870, November 1995.

[SMTP-AUTH] Myers, J., "SMTP Service Extension for Authentication", Work in Progress.

[SMTP-CODES] Vaudreuil, G., "Enhanced Mail System Status Codes", RFC 1893, January 1996.

[SMTP-MTA] Postel, J., "Simple Mail Transfer Protocol", STD 10, RFC 821, August 1982.

Partridge, C., "Mail Routing and the Domain System", STD 14, RFC 974, January 1986.

Braden, R., Editor, "Requirements for Internet Hosts -- Application and Support", STD 3, RFC 1123, October 1989.

12. Authors' Addresses

Randall Gellens
QUALCOMM Incorporated
6455 Lusk Blvd.
San Diego, CA 92121-2779
U.S.A.

Phone: +1 619 651 5115
Fax: +1 619 651 5334
EMail: Randy@Qualcomm.Com

John C. Klensin
MCI Telecommunications
800 Boylston St, 7th floor
Boston, MA 02199
USA

Phone: +1 617 960 1011
EMail: klensin@mci.net

13. Full Copyright Statement