Internet Engineering Task Force (IETF)
Request for Comments: 6409
STD: 72
Obsoletes: 4409
Category: Standards Track
ISSN: 2070-1721

R. Gellens
QUALCOMM Incorporated
J. Klensin

November 2011

Message Submission for Mail

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 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.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6409.

Table of Contents

1. Introduction

SMTP [SMTP-MTA] 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 that 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 have 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, due to the prevalence of machines that have worms, viruses, or other malicious software that generate large amounts of spam, many sites now prohibit outbound traffic on the standard SMTP port (port 25), funneling all mail submissions through submission servers.

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 the Message Format specification [MESSAGE-FORMAT] and related 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 (e.g., 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, e.g., to conceal local name or address spaces. 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 do the following 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.

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

2. Document Information

2.1. Definitions of Terms Used in This Memo

Many of the concepts and terms used in this document are defined in [SMTP-MTA]; familiarity with those documents is assumed here.

Fully Qualified

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

Message Submission Agent (MSA)

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

Message Transfer Agent (MTA)

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

Message User Agent (MUA)

A process that acts (often on behalf of a user and with a user interface) to compose and submit new messages, and to process delivered messages.

For delivered messages, the receiving MUA may obtain and process the message according to local conventions or, in what is commonly referred to as a split-MUA model, Post Office Protocol [POP3] or IMAP [IMAP4] is used to access delivered messages, whereas the protocol defined here (or SMTP) is used to submit messages.

2.2. Conventions Used in This Document

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], with additional restrictions or allowances as specified here.

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

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 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 that 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 other tunnels, 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, one that is not tied to other protocols.

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

Secure IP [IPSEC], and other encrypted and authenticated tunneling techniques, can also be used and provide additional benefits of protection against eavesdropping and traffic analysis.

Requiring a POP [POP3] authentication (from the same IP address) within some amount of time (e.g., 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, RCPT, 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, RCPT, or DATA command that contains improper domain references.

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

4.3. Require Authentication

The MSA MUST, by default, issue an error response to the MAIL 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 any 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 or RCPT 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 denial-of-service (DoS) attacks.

5.3. Apply Shorter Timeouts

The timeouts specified in Section 4.5.3.2 of RFC 5321 [SMTP-MTA] are designed to deal with the many types of situations that can be encountered on the public Internet. The relationship among clients and servers corresponding to this specification is typically much closer and more predictable. Submission clients behave differently from relay client in some areas, especially tolerance for timeouts. In practice, message submission clients tend to have short timeouts (perhaps 2-5 minutes for a reply to any command). Submission servers SHOULD respond to any command (even DATA) in fewer than 2 minutes.

When the submission server has a close administrative and/or network relationship with the submission client(s) -- e.g., with a webmail interface calling on a tightly bound submission server -- mutual agreement on much shorter timeouts MAY be appropriate.

6. Optional Actions

The MSA MAY do any of the following.

6.1. Enforce Submission Rights

The MSA MAY issue an error response to a MAIL 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 a RCPT 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, 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.

6.5. Adjust Character Encodings

Subject to limits imposed by other protocols and specifications, the MSA MAY convert among character sets or string encodings to improve message usefulness, likelihood of delivery, or conformance with other specifications or recommendations. Such conversions MAY include, when necessary, replacement of addresses whose encoding does not conform to RFC 5321 with ones that do, using information available out of band.

7. Interaction with SMTP Extensions

The following table lists Standards Track and Experimental SMTP extensions whose documents do not explicitly specify their applicability to this protocol. Listed are the EHLO keyword, name, an indication as to the use of the extension on the submit port, and a reference.

Keyword	Name	Sub-mission	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	[REPLY-521]
CHECKPOINT	Checkpoint/Restart	MAY	[CHECKPOINT]
BINARYMIME	Binary MIME	MAY	[CHUNKING]
CHUNKING	Chunking	MAY	[CHUNKING]
8BITMIME	Use 8-bit data	SHOULD	[RFC6152]
AUTH	Authentication	MUST	[SMTP-AUTH]
STARTTLS	Start TLS	MAY	[START-TLS]
NO-SOLICITING	Notification of no soliciting	MAY	[RFC3865]
MTRK	Message Tracking	MAY	[MSG-TRACK]
ATRN	On-Demand Relay	MUST NOT	[RFC2645]
DELIVERBY	Deliver By	MAY	[RFC2852]
CONPERM	Content Conversion Permission	MAY	[RFC4141]
CONNEG	Content Conversion Negotiation	MAY	[RFC4141]

Table 1

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 to unauthenticated senders than is needed.

[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.

[START-TLS] is the most widely used mechanism, at the time this document was written, that allows the MUA and MSA to protect message submission integrity and privacy.

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 that 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.

Any message forwarded or delivered by the MSA MUST conform to the requirements of [SMTP-MTA] and [MESSAGE-FORMAT] or the requirements permitted by extensions that are supported by the MSA and accepted by the next-hop server.

Message modification can affect the validity of an existing message signature, such as by DomainKeys Identified Mail (DKIM) [DKIM], Pretty Good Privacy (PGP) [RFC4880], or Secure MIME (S/MIME) [RFC5751], and can render the signature invalid. This, in turn, can affect message handling by later receivers, such as filtering engines that consider the presence or absence of a valid signature.

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, for example, 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 and rewrite aliases (e.g., Canonical Name (CNAME) records) for domain names, in the SMTP envelope and/or in address fields of the header, subject to local policy.

NOTE: SMTP [SMTP-MTA] prohibits the use of domain name aliases in addresses and the session-opening announcement. As with other SMTP requirements, RFC 5321 effectively prohibits an MSA from forwarding such messages into the public Internet. Nonetheless, 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 that 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 that strips the leftmost element of the domain, if the complete domain matches '*.foo.example.net', would be acceptable.

The MSA MUST NOT rewrite a forward-pointing (destination) address in a way that violates the constraints of [SMTP-MTA] on modifications of local-parts. Changes to addressing and encoding, carried out in conjunction with the action of Section 6.5, do not violate this principle if the MSA has sufficient information available to successfully and accurately apply the substitution.

9. Security Considerations

Separation of submission and relay of messages allows a site to implement different policies for the two types of services, including requiring the use of additional security mechanisms for one or both. It can do this in a way that 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 commands 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 entries in Table 1 have been corrected (reference for NO-SOLICITING) and extended (ATRN, DELIVERBY, CONPERM, and CONNEG). The "SMTP Service Extensions" registry has been updated to reflect the changed and new entries. Entries in the registry that do not appear in the table above are correct and should not be altered.

The entry in the "SMTP Service Extensions" registry for RFC 4409 has been updated to reference this document. The original reference for Submit (RFC 2476), which should have been corrected earlier, has also been updated to point to this document.

The entry in the "Service Name and Transport Protocol Port Number Registry" for port 587 has been updated to point to this document.

11. Acknowledgments

The preparation and development of the current version of this specification was stimulated by discussions in the IETF YAM and EAI Working Groups. Dave Crocker, Subramanian Moonesamy, Barry Leiba, John Levine, and others provided text that appeared in this document or versions leading up to it.

Nathaniel Borenstein and Barry Leiba were instrumental in the development of RFC 4409, the update to RFC 2476.

The original memo (RFC 2476) was developed, in part, based on comments and discussions that took place on and off the IETF-Submit

mailing list. The help of those who took the time to review that document 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. References

12.1. Normative References

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

[SMTP-AUTH] Siemborski, R. and A. Melnikov, "SMTP Service Extension for Authentication", RFC 4954, July 2007.

[SMTP-MTA] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, October 2008.

12.2. Informative References

[CHECKPOINT] Crocker, D. and N. Freed, "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 3030, December 2000.

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

[DKIM] Crocker, D., Hansen, T., and M. Kucherawy, "DomainKeys Identified Mail (DKIM) Signatures", RFC 6376, September 2011.

[DSN] Moore, K., "Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)", RFC 3461, January 2003.

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

[IMAP4] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1", RFC 3501, March 2003.

[IPSEC] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[MESSAGE-FORMAT]
Resnick, P., Ed., "Internet Message Format", RFC 5322, October 2008.

[MSG-TRACK] Allman, E. and T. Hansen, "SMTP Service Extension for Message Tracking", RFC 3885, September 2004.

[PIPELINING] Freed, N., "SMTP Service Extension for Command Pipelining", STD 60, RFC 2920, September 2000.

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

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

[RFC2645] Gellens, R., "ON-DEMAND MAIL RELAY (ODMR) SMTP with Dynamic IP Addresses", RFC 2645, August 1999.

[RFC2852] Newman, D., "Deliver By SMTP Service Extension", RFC 2852, June 2000.

[RFC3865] Malamud, C., "A No Soliciting Simple Mail Transfer Protocol (SMTP) Service Extension", RFC 3865, September 2004.

[RFC4141] Toyoda, K. and D. Crocker, "SMTP and MIME Extensions for Content Conversion", RFC 4141, November 2005.

[RFC4880] Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R. Thayer, "OpenPGP Message Format", RFC 4880, November 2007.

[RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", RFC 5751, January 2010.

[RFC6152] Klensin, J., Freed, N., Rose, M., and D. Crocker, "SMTP Service Extension for 8-bit MIME Transport", STD 71, RFC 6152, March 2011.

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

[SMTP-CODES] Vaudreuil, G., "Enhanced Mail System Status Codes", RFC 3463, January 2003.

[START-TLS] Hoffman, P., "SMTP Service Extension for Secure SMTP over Transport Layer Security", RFC 3207, February 2002.

Appendix A. Major Changes from RFC 4409

The protocol specified by this document is not substantively different from that of RFC 4409. However, the present specification contains several clarifications and updates to reflect changes and revisions to other documents subsequent to the publication of RFC 4409. The following specific changes may be of interest to some readers.

- Updated several references to reflect more recent versions of the various specifications. As part of this, reclassified RFC 4954 to a normative reference (SMTP AUTH is a MUST for RFC 4409 and this specification).
- Updated the text in Section 7 to reflect the existence and partial population of the registry and the included table (Table 1) to correct one entry and add others. See Section 10 for more information.
- Added new text (Section 5.3) to clarify that Submission Servers should respond quickly.
- Added text to make it explicit that character encoding changes are permitted.
- Added text to make it clear that modifications to signed messages may cause problems and that they should be carefully considered.

Authors' Addresses

Randall Gellens
QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, CA 92121-2779
USA

EMail: rg+ietf@qualcomm.com

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

Phone: +1 617 491 5735
EMail: john-ietf@jck.com