Internet Draft
draft-ietf-msgtrk-smtpext-05.txt
Valid for six months
Updates: RFC 1891

E. Allman
Sendmail, Inc.
T. Hansen
AT&T Laboratories

March 19, 2003

SMTP Service Extension for Message Tracking

<draft-ietf-msgtrk-smtpext-05.txt>

Status of This Memo

This document is a submission by the MSGTRK Working Group of the Internet Engineering Task Force (IETF). Comments should be submitted to the ietf-msgtrk@imc.org mailing list. An archive of the mailing list may be found at

http://www.imc.org/ietf-msgtrk/index.html

Distribution of this memo is unlimited.

1. Abstract

This memo defines an extension to the SMTP service whereby a client may mark a message for future tracking.

2. Other Documents and Conformance

The model used for Message Tracking is described in [DRAFT-MTRK-MODEL].

Doing a Message Tracking query is intended as a "last resort" mechanism. Normally, Delivery Status Notifications (DSNs) [RFC-DSN-SMTP] and Message Disposition Notifications (MDNs) [RFC-MDN] would provide the primary delivery status. Only if the message is not received, or there is no response from either of these mechanisms should a Message Tracking query be issued.

The definition of the base64 token is imported from section 6.8 of [RFC-MIME]. Formally,

```
base64 =  %2b / %2f / %x30-39 / %x41-5a / %x61-7a
```

The definition of the DIGIT token is imported from [RFC-MSGFMT]. Formally,

```
DIGIT =       %x30-39
```

Syntax notation in this document conforms to [RFC-ABNF].

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 RFC 2119 [RFC-KEYWORDS].

3. SMTP Extension Overview

The Message Tracking SMTP service extension uses the SMTP service extension mechanism described in [RFC-ESMTP]. The following service extension is hereby defined:

(1) The name of the SMTP service extension is "Message Tracking".

(2) The EHLO keyword value associated with this extension is "MTRK".

(3) No parameters are allowed with this EHLO keyword value. Future documents may extend this specification by specifying parameters to this keyword value.

(4) One optional parameter using the keyword "MTRK" is added to the MAIL command. In addition, the ENVID parameter of the MAIL command (as defined in RFC 1891 sections 5.4) MUST be supported, with extensions as described below. The ORCPT parameter of the RCPT command (as defined in RFC 1891 section 5.2) MUST also be supported. All semantics associated with ENVID and ORCPT described in RFC 1891 MUST be supported as part of this extension.

(5) The maximum length of a MAIL command line is increased by 40 characters by the possible addition of the MTRK keyword and value. Note that the 507 character extension of RCPT commands for the ORCPT parameter and the 107 character extension of MAIL commands for the ENVID parameter as mandated by RFC 1891 [RFC-DSN-SMTP] must also be included.

(6) No SMTP verbs are defined by this extension.

4. The Extended MAIL Command

The extended MAIL command is issued by an SMTP client when it wishes to inform an SMTP server that message tracking information should be retained for future querying. The extended MAIL command is identical to the MAIL command as defined in [RFC-SMTP], except that MTRK, ORCPT, and ENVID parameters appear after the address.

4.1. The MTRK parameter to the ESMTP MAIL command

Any sender wishing to request the retention of data for further tracking of message must first tag that message as trackable by creating two values A and B:

A = some-large-random-number
B = SHA1(A)

The large random number A is calculated on a host-dependent basis. See [RFC-RANDOM] for a discussion of choosing good random numbers. This random number MUST be at least 128 bits

but MUST NOT be more than 1024 bits.

The 128-bit hash B of A is then computed using the SHA-1 algorithm as described in [NIST-SHA1].

The sender then base64 encodes value B and passes that value as the mtrk-certifier on the MAIL command:

```
mtrk-parameter  = "MTRK=" mtrk-certifier [ ":" mtrk-timeout ]
mtrk-certifier  = base64        ; authenticator
mtrk-timeout    = 1*9DIGIT      ; seconds until timeout
```

A is stored in the originator's tracking database to validate future tracking requests as described in [DRAFT-MTRK-MTQP]. B is stored in tracking databases of compliant receiver MTAs and used to authenticate future tracking requests.

The mtrk-timeout field indicates the number of seconds that the client requests that this tracking information be retained on intermediate servers, as measured from the initial receipt of the message at that server. Servers MAY ignore this value if it violates local policy. In particular, servers MAY silently enforce an upper limit to how long they will retain tracking data; this limit MUST be at least one day.

If no mtrk-timeout field is specified then the server should use a local default. This default SHOULD be 8-10 days and MUST be at least one day. Notwithstanding this clause, the information MUST NOT be expired while the message remains in the queue for this server: that is, an MTQP server MUST NOT deny knowledge of a message while that same message sits in the MTA queue.

If the message is relayed to another compliant SMTP server, the MTA acting as the client SHOULD pass an mtrk-timeout field equal to the remaining life of that message tracking information. Specifically, the tracking timeout is decremented by the number of seconds the message has lingered at this MTA and then passed to the next MTA. If the decremented tracking timeout is less than or equal to zero, the entire MTRK parameter MUST NOT be passed to the next MTA; essentially, the entire tracking path is considered to be lost at that point.

See [RFC-DELIVERYBY] section 4 for an explanation of why a timeout is used instead of an absolute time.

4.2. Use of ENVID

To function properly, Message Tracking requires that each message have a unique identifier that is never reused by any other message. For that purpose, if the MTRK parameter is given, an ENVID parameter MUST be included, and the syntax of ENVID from RFC 1891 section 5.4 is extended as follows:

```
envid-parameter = "ENVID=" unique-envid
unique-envid    = local-envid "@" fqhn
```

```
    local-envid     = xtext
    fqhn            = xtext
```

The unique-envid MUST be chosen in such a way that the same ENVID will never be used by any other message sent from this system or any other system. In most cases, this means setting fqhn to be the fully qualified host name of the system

generating this ENVID, and local-envid to an identifier that is never re-used by that host.

In some cases, the total length of (local-envid + fqhn + 1) (for the `@' sign) may exceed the total acceptable length of ENVID (100). In this case, the fqhn SHOULD be replaced by the SHA1(fqhn) encoded into BASE64. After encoding, the 160 bit SHA-1 will be a 27 octet string, which limits local-envid to 72 octets. Implementors are encouraged to use an algorithm for the local-envid that is reasonably unique. For example, sequential integers have a high probability of intersecting with sequential integers generated by a different host, but a SHA-1 of the current time of day concatenated with the host's IP address and a random number are unlikely to intersect with the same algorithm generated by a different host.

Any resubmissions of this message into the message transmission system MUST assign a new ENVID. In this context, "resubmission" includes forwarding or resending a message from a user agent, but does not include MTA-level aliasing or forwarding where the message does not leave and re-enter the message transmission system.

4.3. Forwarding Tracking Certifiers

MTAs SHOULD forward unexpired tracking certifiers to compliant mailers as the mail is transferred during regular hop-to-hop transfers. If the "downstream" MTA is not MTRK-compliant, then the MTRK= parameter MUST be deleted. If the downstream MTA is DSN-compliant, then the ENVID and ORCPT parameters MUST NOT be deleted.

If aliasing, forwarding, or other redirection of a recipient occurs, and the result of the redirection is exactly one recipient, then the MTA SHOULD treat this as an ordinary hop-to-hop transfer and forward the MTRK=, ENVID=, and ORCPT= values; these values MUST NOT be modified except for decrementing the mtrk-timeout field of the MTRK= value, which MUST be modified as described in section 4.1 above.

MTAs MUST NOT copy MTRK certifiers when a recipient is aliased, forwarded, or otherwise redirected and the redirection results in more than one recipient. However, an MTA MAY designate one of the multiple recipients as the "primary" recipient to which tracking requests shall be forwarded; other addresses MUST NOT receive tracking certifiers. MTAs MUST NOT forward MTRK certifiers when doing mailing list expansion.

5. Security Considerations

5.1. Denial of service

An attacker could attempt to flood the database of a server by submitting large numbers of small, tracked messages. In this case, a site may elect to lower its maximum retention period

retroactively.

5.2. Confidentiality

The mtrk-authenticator value (``A'') must be hard to predict and not reused.

The originating client must take reasonable precautions to protect the secret. For example, if the secret is stored in a message store (e.g., a "Sent" folder), the client must make sure the secret isn't accessible by attackers, particularly on a shared store.

Many site administrators believe that concealing names and topologies of internal systems and networks is an important security feature. MTAs need to balance such desires with the need to provide adequate tracking information.

In some cases site administrators may want to treat delivery to an alias as final delivery in order to separate roles from individuals. For example, sites implementing ``postmaster'' or ``webmaster'' as aliases may not wish to expose the identity of those individuals by permitting tracking through those aliases. In other cases, providing the tracking information for an alias is important, such as when the alias points to the user's preferred public address.

Therefore, implementors are encouraged to provide mechanisms by which site administrators can choose between these alternatives.

6. IANA Considerations

IANA is to register the SMTP extension defined in section 3.

7. Acknowledgements

Several individuals have commented on and enhanced this draft, including Philip Hazel, Alexey Melnikov, Lyndon Nerenberg, Chris Newman, and Gregory Neil Shapiro.

8. Normative References

[DRAFT-MTRK-MODEL]
T. Hansen, ``Message Tracking Model and Requirements.'' draft-ietf-msgtrk-model-03.txt. November 2000.

[DRAFT-MTRK-MTQP]
T. Hansen, ``Message Tracking Query Protocol.'' draft-ietf-msgtrk-mtqp-01.txt. November 2000.

[RFC-ABNF]
Crocker, D., Editor, and P. Overell, ``Augmented BNF for

Syntax Specifications: ABNF'', RFC 2234, November 1997.

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

[RFC-KEYWORDS]
S. Bradner, ``Key words for use in RFCs to Indicate Requirement Levels.'' RFC 2119. March 1997.

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

[NIST-SHA1]
NIST FIPS PUB 180-1, ``Secure Hash Standard.'' National Institute of Standards and Technology, U.S. Department of Commerce. May 1994. DRAFT.

[RFC-SMTP]
J. Klensin, editor, ``Simple Mail Transfer Protocol.'' RFC 2821. April 2001.

9. Informational References

[RFC-DELIVERYBY]
D. Newman, ``Deliver By SMTP Service Extension.'' RFC 2852. June 2000.

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

[RFC-MDN]
R. Fajman, ``An Extensible Message Format for Message Disposition Notifications.'' RFC 2298. March 1998.

[RFC-RANDOM]
D. Eastlake, S. Crocker, and J. Schiller, ``Randomness Recommendations for Security.'' RFC 1750. December 1994.

10. Authors' Addresses

Eric Allman
Sendmail, Inc.

6425 Christie Ave, 4th Floor
Emeryville, CA 94608
U.S.A.

E-Mail: eric@Sendmail.COM
Phone: +1 510 594 5501
Fax: +1 510 594 5429

Tony Hansen
AT&T Laboratories
Middletown, NJ 07748
U.S.A.

Phone: +1 732 420 8934
E-Mail: tony@att.com