Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 8 January 2026

A. Robinson
Google Inc.

7 July 2025

DKIM2 Procedures for bounce processing
draft-robinson-dkim2-bounce-processing-01

Abstract

This memo provides a description of the procedures for bounce processing that should be performed by any mail system that implements DKIM2, as part of the overall DKIM2 protcol definition.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on 8 January 2026.

Copyright Notice

Table of Contents

1. Introduction

As part of the DKIM2 protocol, handling for Delivery Status Notifications (DSNs, defined in [RFC3461]) is necessary to ensure that systems receiving these notifications have a mechanism to both authenticate the contents of the DSN, and to determine if the system generating the DSN is authorized to do so for the message being returned.

2. Bounce processing

2.1. Forward path

At a high level, the forward path in DKIM2 involves the addition of a new DKIM2 header field by each system that handles a message. This header field declares that the message was originated by a system that has the right to do so, either because that system is the origin of the message, or because the system received the message from somewhere else and has decided to forward it to another system. In order to support injection-resistant bounce handling, each system must record in the DKIM2 header field's mf= tag the [RFC5321] return-path mailbox for the message, along with all other values as required by the DKIM2 protocol.

The return-path mailbox for an incoming message should be the address included in the [RFC5321] transaction's MAIL FROM command. This identity will be related to the last (highest i= value) DKIM2 signature in the message, so this address represents an authenticated destination for future bounce notifications related to the message.

2.2. Return path

2.2.1. Bounce origination

Once a system decides that a bounce notification needs to be generated in response to a message that it previously accepted for delivery, a new message must be formed to notify the sender that the message was not delivered successfully. Per [RFC3461], the bounce notification message has a top-level MIME part of type multipart/report. Among other things, that MIME part must contain a MIME part of type message/rfc822 that holds either the original message exactly as it was submitted by the sending system or just the header for that message, so that the receiver of the bounce notification can authenticate the signatures associated with the original message before processing the bounce notification.

2.2.2. Bounce propagation

A system that acts as an intermediary step for the handling of a message in the forward path may decide to propagate bounce notifications through the return path of the message in response to receiving a bounce notification.

Same as the initial DSN, the intermediary system’s generated bounce notification message must contain a MIME part of type message/report with a sub-part of type message/rfc822 that holds the original message or its header.

The bounce notification must be sent to the return-path mailbox listed in the previous system’s DKIM2 header field.

An intermediary system must be able to recover at least the originally-submitted header for a forwarded message, for the purposes of generating bounce notifications. These systems may choose to use the DKIM2 modifications they declared as part of the forward path to reconstruct the original message based on the inbound bounce notification, if it is desirable to return the full message and the inbound bounce notification also includes the full message. Forwarding systems that want to return the full message in all cases should retain the content required to do that as it is not guaranteed to be present in a received DSN.

2.2.3. Authentication of inbound bounce notifications

When a system receives a DKIM2 signed bounce notification, and the included original message is also DKIM2 signed, the bounce receiver should verify that the original message was not altered. This means:

1) The DSN’s DKIM2 signature must have a signing domain that is aligned with the recipient of the message that is being returned. The recipient’s address is located in the rt= tag of the last (highest i= tag) DKIM2-Signature in the returned message. 1) The last (highest i= tag) DKIM2 header field of the returned message must be one that was generated by the system receiving the bounce notification, determined by examining the d= and mf= tags of that signature header field. 1) The signature in that DKIM2 header field must match the contents of the returned message. Verifiers must handle truncated or missing original message bodies gracefully, by using the body hash value included in the signature header field without comparing it to the body contents.

The exact details of how to perform DKIM2 signature validation are out of scope for this draft.

In the event that the bounce notification contains unauthenticated content, the bounce receiver may decide to deem the bounce message itself as malicious and not propagate it through the return path declared in that message.

2.2.4. DKIM2 signing of bounce notifications

Bounce notifications should be DKIM2 signed in exactly the same way as a newly-originated message. This signature must use i=1 since the system generating the notification is the originator of that message, and include an empty mf= tag to align with the SMTP transaction delivering the DSN.

2.3. Example

The following is a very simplified description of the SMTP transactions involved in the forward and return paths for a message. Only the SMTP commands and header fields related to DKIM2 bounce processing are mentioned.

Message origination from example.com to foo.com:

‘‘‘ MAIL FROM: original@example.com (mailto:original@example.com) RCPT TO: dest@foo.com (mailto:dest@foo.com) DATA DKIM2: i=1; d=example.com; mf=original@example.com; rt=dest@foo.com From: Sender original@example.com (mailto:original@example.com) To: dest@foo.com

I hope this email reaches its destination . ‘‘‘

Forwarding of the message from foo.com to bar.com:

‘‘‘ MAIL FROM: something@foo.com (mailto:something@foo.com) RCPT TO: dest@bar.com (mailto:dest@bar.com) DATA DKIM2: i=2; d=foo.com; mf=something@foo.com; rt=newdest@bar.com DKIM2: i=1; d=example.com; mf=original@example.com; rt=dest@foo.com From: Sender original@example.com (mailto:original@example.com) To: dest@foo.com

I hope this email reaches its destination . ‘‘‘

Bounce notification from bar.com to foo.com:

‘‘‘ MAIL FROM: <> RCPT TO: something@foo.com (mailto:something@foo.com) DATA DKIM2: i=1; d=bar.com; rt=something@foo.com From: postmaster@bar.com (mailto:postmaster@bar.com) To: something@foo.com (mailto:something@foo.com) Subject: DSN for ... Content-Type: multipart/report; boundary="divider43541325151"

--divider43541325151 Content-Type: text/plain

This message is being returned.

--divider43541325151 Content-Type: message/delivery-status

--divider43541325151 Content-Type: message/rfc822 DKIM2: i=2; d=foo.com; mf=something@foo.com; rt=newdest@bar.com DKIM2: i=1; d=example.com; mf=original@example.com; rt=dest@foo.com From: Sender original@example.com (mailto:original@example.com) To: dest@foo.com

I hope this email reaches its destination --divider43541325151-- . ‘‘‘

Propagated bounce notification from foo.com to example.com:

‘‘‘ MAIL FROM: <> RCPT TO: original@example.com (mailto:original@example.com) DATA DKIM2: i=1; d=foo.com; rt=original@example.com From: postmaster@foo.com (mailto:postmaster@foo.com) To: original@example.com (mailto:original@example.com) Subject: DSN for ... From: Sender original@example.com (mailto:original@example.com) To: dest@foo.com Content-Type: multipart/report; boundary="divider89869878"

--divider89869878 Content-Type: text/plain

This message is being returned.

--divider89869878 Content-Type: message/delivery-status

```
--divider43541325151 Content-Type: message/rfc822 DKIM2: i=1;
d=example.com; mf=original@example.com; rt=dest@foo.com From: Sender
original@example.com (mailto:original@example.com) To: dest@foo.com

I hope this email reaches its destination --divider89869878-- . ‘‘‘
```

2.4. Security considerations

To be covered in primary DKIM2 document.

2.5. IANA considerations

To be covered in primary DKIM2 document.

3. Normative References

[RFC3461] Moore, K., "Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)", RFC 3461, DOI 10.17487/RFC3461, January 2003, <https://www.rfc-editor.org/rfc/rfc3461>.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <https://www.rfc-editor.org/rfc/rfc5321>.

Appendix A. Changes from Earlier Versions

v01:

* updated example syntax to match dkim2-headers document

[[This section to be removed by RFC Editor]]

Author’s Address

Allen Robinson
Google Inc.
Email: arobins@google.com