Network Working Group
Internet-Draft
Intended status: Informational
Expires: 1 January 2026

A. Robinson
Google Inc.
T. Herkula
1&1 Mail & Media GmbH

30 June 2025

DKIM2 Message Examples
draft-robinson-dkim2-message-examples-00

Abstract

This memo provides examples of how DKIM2 would apply to common email usage scenarios.

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 1 January 2026.

Table of Contents

1. DKIM2 Message Examples 2
1.1. Introduction 2
1.2. Document Conventions 2
1.3. Scenarios 3
1.3.1. Direct delivery 3
1.3.2. Autoforwarding (no alteration) 4
1.3.3. Mailing list (no alteration) 5
1.3.4. Mailing list (with alteration) 6
1.3.5. Mailing list (with alteration and From munging) . . . 7
1.3.6. Sending on behalf of another domain 8
1.4. IANA Considerations 9
1.5. Security Considerations 9
2. Normative References 9
Appendix A. Changes from Earlier Versions 9
Authors' Addresses 9

1. DKIM2 Message Examples

1.1. Introduction

This draft provides a collection of email message scenarios, along with the proposed way that DKIM2 could operate under those scenarios.

1.2. Document Conventions

Terminology from [RFC5598] is used extensively throughout this document.

* "Transaction" represents an interaction between two ADMDs.

* "Origin" refers to the first ADMD involved in the delivery of the message.

* "Destination" refers to the final ADMD involved in the delivery of the message.

* "DKIM2-Signature" as the header field name is a placeholder. The standardization process will involve coming to consensus on a name for the field.

* DKIM2-Signature field values will not contain the bh= tag.

* DKIM2-Signature field values will contain a simplified b= tag, where "PASS" means the signature can be verified against the message as-is, "PASS_AFTER_UNDO_MODS" means pass after applying DKIM2 modification algebra to the message, and "FAIL" means an unrecoverable signature.

* DKIM2-Modification is a human-consumable description of the changes, in lieu of having a rough definition of what the machine-consumable modification algebra should look like.

* DKIM-Signature header fields are not included. These can safely be present in DKIM2 messages, but do not contribute to the DKIM2-oriented handling of a message.

* The destination address header fields 5322.To, 5322.Cc, 5322.Bcc are left out. These are not relevant to DKIM2, since there is no requirement that 5321.To have any relationship to the values contained in those header fields.

* Other mandatory [RFC5322] headers fields that aren’t relevant to DKIM2 processing will also be left out.

* "Alignment" needs further definition in the context of DKIM2, but for now it is being used with the same meaning as DMARC alignment, as defined in [RFC7489].

* ==== delimiters are used to indicate the start and end of the SMTP ([RFC5321]) transaction, and are not part of the transaction’s content.

1.3. Scenarios

1.3.1. Direct delivery

This is the common case for email. The initial ADMD has a message to be delivered somewhere, and the ADMD that is on the receiving end of that SMTP transaction is that message’s final destination.

Transaction: Origin to destination

```
====
MAIL FROM: <a@origin.example>
RCPT TO: <b@destination.example>
DATA
DKIM2-Signature: i=1; d=origin.example; s=key1; mf=a@origin.example;
    rt=b@destination.example; b=PASS
From: <a@origin.example>

A Message!
====
```

In the initial transaction of a DKIM2 signed message, the signing domain must be aligned with the domain in 5322.From. Note that the mf= and 5321.MailFrom are equal, but they do not need to be equal to the 5322.From.

In every DKIM2 transaction, it is required that the topmost (highest i=) DKIM2-Signature’s signing domain be aligned with the domain in that signature’s mf= tag, and that the mf= tag be equal to the 5321.MailFrom for that transaction. Alignment of these domains is a mitigation for backscatter, and it is left to the system operator to prevent local backscatter (ex. acct1@example.com misusing 5321.MailFrom of acct2@example.com).

In every DKIM2 transaction, it is required that the topmost DKIM2-Signature’s rt= be equal to the 5321.RcptTo for that transaction. This equality is a mitigation for message replay, by making delivery to any other mailbox (even at the same host) be not authenticated by DKIM2. Acceptance of messages that don’t authenticate with DKIM2 is a matter of local policy.

1.3.2. Autoforwarding (no alteration)

This is often called the "alumni forwarder" scenario, but many other forwarding services exist. An ADMD has a message to send, and the destination is an address at another ADMD acting as a forwarding service. The forwarding service resends the message to another ADMD, which is the final destination for the message.

In this scenario, it is assumed that the forwarding service does not alter the message at all.

Transaction: Origin to forwarder

```
====
MAIL FROM: <a@origin.example>
RCPT TO: <b@alias.example>
DATA
DKIM2-Signature: i=1; d=origin.example; s=key1; mf=a@origin.example;
    rt=b@alias.example; b=PASS
From: <a@origin.example>

A Message!
====
```

Transaction: Forwarder to destination

```
====
MAIL FROM: <b@alias.example>
RCPT TO: <c@destination.example>
DATA
DKIM2-Signature: i=2; d=alias.example; s=key4321; mf=b@alias.example;
    rt=c@destination.example; b=PASS
DKIM2-Signature: i=1; d=origin.example; s=key1; mf=a@origin.example;
    rt=b@alias.example; b=PASS
From: <a@origin.example>

A Message!
====
```

In the forwarding transaction, the i=2 signing domain is aligned to the 5321.MailFrom and the domain in i=1 rt=. There is no requirement that i=2 signing be aligned with 5322.From.

DMARC requirements can be satisfied in both transactions, because there is a passing signature aligned with the 5322.From.

1.3.3. Mailing list (no alteration)

This operates like an autoforwarder. The only difference is that these systems are expected to re-deliver to multiple destinations instead of just one.

Transaction: Origin to mailing list

```
====
MAIL FROM: <a@origin.example>
RCPT TO: <m@list.example>
DATA
DKIM2-Signature: i=1; d=origin.example; s=key1; mf=a@origin.example;
    rt=m@list.example; b=PASS
From: <a@origin.example>

A Message!
====

Transaction: Mailing list to destination

====
MAIL FROM: <m@list.example>
RCPT TO: <b@subscriber.example>
DATA
DKIM2-Signature: i=2; d=list.example; s=key50; mf=m@list.example;
    rt=b@subscriber.example; b=PASS
DKIM2-Signature: i=1; d=origin.example; s=key1; mf=a@origin.example;
    rt=m@list.example; b=PASS
From: <a@origin.example>

A Message!
====
```

1.3.4. Mailing list (with alteration)

Similar to the non-modifying mailing list case, but with modifications of the message (body, 5322.Subject, etc.) that invalidate the signature in i=1.

```
Transaction: Origin to mailing list

====
MAIL FROM: <a@origin.example>
RCPT TO: <m@list.example>
DATA
DKIM2-Signature: i=1; d=origin.example; s=key1; mf=a@origin.example;
    rt=m@list.example; b=PASS
From: <a@origin.example>

A Message!
====

Transaction: Mailing list to destination
```

```
====
MAIL FROM: <m@list.example>
RCPT TO: <b@subscriber.example>
DATA
DKIM2-Signature: i=2; d=list.example; s=key1; mf=m@list.example;
    rt=b@subscriber.example; b=PASS
DKIM2-Modification: i=2; delta="Appended a line"
DKIM2-Signature: i=1; d=origin.example; s=key50; mf=a@origin.example;
    rt=m@list.example; b=PASS_AFTER_UNDO_MODS
From: <a@origin.example>

A Message!
Click https://list.example/unsubscribe to unsubscribe from this.
====
```

It is unclear whether the second transaction can be considered to satisfy origin.example's DMARC requirements, as origin.example's signature did not pass on the message as presented.

1.3.5. Mailing list (with alteration and From munging)

Further modification, where the mailing list also changes the 5322.From header field to something else. This is done in today's ecosystem to allow for delivery of modified messages sent from domains with DMARC policies.

Transaction: Origin to mailing list

```
====
MAIL FROM: <a@origin.example>
RCPT TO: <m@list.example>
DATA
DKIM2-Signature: i=1; d=origin.example; s=key1; mf=a@origin.example;
    rt=m@list.example; b=PASS
From: <a@origin.example>

A Message!
====
```

Transaction: Mailing list to destination

```
====
MAIL FROM: <m@list.example>
RCPT TO: <b@subscriber.example>
DATA
DKIM2-Signature: i=2; d=list.example; s=key1; mf=m@list.example;
    rt=b@subscriber.example; b=PASS
DKIM2-Modification: i=2;
    delta="Appended a line; From used to be "a@origin.example""
DKIM2-Signature: i=1; d=origin.example; s=key50; mf=a@origin.example;
    rt=m@list.example; b=PASS_AFTER_UNDO_MODS
From: "a via list" <m@list.example>

A Message!
Click https://list.example/unsubscribe to unsubscribe from this.
====
```

DMARC is satisfied by this message. There is a signature from the domain of 5322.From that passes on the message being presented, and the original 5322.From isn’t visible unless the receiving system decides that that’s an appropriate thing to do.

It should be required that any changes 5322.From be included in a signature where the signing domain aligns with the new 5322.From, similar to how i=1 must align with the message’s original 5322.From.

1.3.6. Sending on behalf of another domain

There are scenarios in which one ADMD is sending messages on behalf of another ADMD. A common example of this is Email Service Providers (ESPs) that send promotional mail on behalf of their customers.

Transaction: Origin to destination

```
====
MAIL FROM: <something@esp.example>
RCPT TO: <abc@destination.example>
DATA
DKIM2-Signature: i=2; d=esp.example; s=espkey;
    mf=something@esp.example; rt=abc@destination.example; b=PASS
DKIM2-SIGNATURE: i=1; d=brand.example; s=brandkey;
    mf=something@brand.example; rt=something@esp.example; b=PASS
From: "Brand coupons" <no-reply@brand.example>

Here are some coupons for our Brand products!
====
```

Despite being originated from the ESP directly, DKIM2's requirement that the i=1 d= tag have alignment with both the 5321.MailFrom and 5322.From means that scenarios like this will require two signatures at origination. The first satisfies the requirement that the signature be aligned with 5322.From, and the second satisfies the requirement that the topmost signature's mf= tag be equal to the 5321.MailFrom of the transaction.

Generation of two signatures is only required when the ESP needs to use a 5321.MailFrom that is not aligned with 5322.From. If this is not required, the mail can be sent using a single signature that aligns with both.

1.4. IANA Considerations

None.

1.5. Security Considerations

Security considerations for DKIM2 will be included in the protocol document.

2. Normative References

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

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, DOI 10.17487/RFC5322, October 2008, <https://www.rfc-editor.org/rfc/rfc5322>.

[RFC5598] Crocker, D., "Internet Mail Architecture", RFC 5598, DOI 10.17487/RFC5598, July 2009, <https://www.rfc-editor.org/rfc/rfc5598>.

[RFC7489] Kucherawy, M., Ed. and E. Zwicky, Ed., "Domain-based Message Authentication, Reporting, and Conformance (DMARC)", RFC 7489, DOI 10.17487/RFC7489, March 2015, <https://www.rfc-editor.org/rfc/rfc7489>.

Appendix A. Changes from Earlier Versions

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

Authors' Addresses

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

Tobias Herkula
1&1 Mail & Media GmbH
Email: tobias.herkula@1und1.de