Workgroup: Network Working Group
Internet-Draft:
draft-vesely-dmarc-mlm-transform-05
Published: 29 June 2022
Intended Status: Experimental
Expires: 31 December 2022
Authors: A. Vesely

Mailing List Manager (MLM) Transformations

Abstract

The widespread adoption of Domain-based Message Authentication, Reporting, and Conformance (DMARC) led Mailing List Managers (MLM) to rewrite the From: header field as a workaround.

This document describes reverting MLM transformations in IETF mailing lists. That way, it is possible to verify DomainKeys Identified Mail (DKIM) signatures that were applied at submission time and thereby restore original identifiers.

For reliable results, some compliance is required of all agents involved, author domain signers, MLMs, forwarders, and final recipients' verifiers.

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 31 December 2022.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of

publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Table of Contents

1. Introduction

As mailing lists do not adhere to an explicitly standardized protocol, their behavior and even their definition vary widely. Their social usage is often paired with web fora, for example. In the IETF standardization process and in some other communities, especially those related to software, instead, the use of terse mailing lists which apply only minimal changes is a radicated tradition. In such environment, mailing list often constitute a key tool to carry out the core work of a group. And, like in any working environment, reciprocal trust is an essential team quality. Therefore, participants authentication is not an irrelevant feature.

Domain-based Message Authentication, Reporting, and Conformance (DMARC) ([RFC7489]) hinges on the alignment of the domain in the From: header field with a verified DKIM signature. For that reason, MLMs that transform messages, however lightly, have to rewrite From:; an operation also known as From: munging.

In this experiment, we try and restore the end-to-end nature of the From: email field after DMARC rewriting, focusing on the behavior of mailing lists of that kind. Several Mailing List Managers (MLMs) are configured to add just a footer and a subject tag to the messages that they redistribute. Although that behavior slightly exceeds the very limited set of modifications and actions described by Section 3.9.2 of [RFC5321], it is a welcome, time-honored tradition. According to their configuration, the modifications they carry out on messages result in a set of stylized transformations that are programmatically revertible. Reversion allows to verify DomainKeys Identified Mail (DKIM) signatures ([RFC6376]) that were applied before the transformation.

Mailbox providers can configure their mail submission agents (MSAs) in order to ease MLM transformation reversion. Or they can make it impossible by signing too many header fields. Their will is expressed by their DKIM signing policy.

At the receiver, the DKIM verifier needs a substantial enhancement to undo the transformations and verify the original signatures. That undoing is carried out in the same way as canonicalization; that is, it does not actually change the message except for adding Authentication-Results: header fields. Details are outlined in Section 4.

So, if submitters sign lightly, MLM operate just minimal changes, and receivers attempt undoing MLM transformation, it is possible to overcome From: munging. The effect is twofold:

1. Author domains receive positive feedback about DKIM verification of mailing list traffic. That might eventually lead them to harden their DMARC policy. (Otherwise, some author domain operators publish p=quarantine; pct=0 to force From: munging by MLM who don't do it when p=none. That way they don't see MLM traffic at all, including errors.)

2. Final recipient's mail delivery agents (MDAs), which know by the Authentication-Results: field whether a rewritten From: header was verified, can safely undo From: rewriting (after any external forwarding). That way, the annoyance causes by munging to end recipients is avoided. MLM transformation reversion reduces DMARC's effects on indirect mail flows.

2. Terms Definitions

Signers and **verifiers** are defined in [RFC6376]. The use of the term **Mailing List Manager**, almost always abbreviated **MLM** follows [RFC6377]. A MLM is a kind of **Mediator** in [RFC5598] parlance.

Message is defined in [RFC5322]. It consists of a **header** made up of one or more **fields** and a **body**, possibly composed of various MIME **entities**, the latter being defined in [RFC2045] and companions.

The term **original** is used here to refer to the Author or parts of the Author's message as it was sent out by the Author's domain, where **Author** is defined in [RFC5598] and [RFC9057].

3. Revertible Transformations

Message modifications can affect the header and/or the body of a message. This document only considers a very limited set of transformations, described in the following subsections. They turn out to be revertible.

3.1. Header Transformations

3.1.1. Subject

MLM often modify the Subject: field by inserting a tag at the beginning of its value. A tag consists of a short text delimited by square brackets. For example:

```
Subject: [added tag] Original value of subject
```

This transformation is easily reverted by removing the tag. For security reasons, subject tags must not exceed 20 characters.

Note that some MLMs carry out further changes to this field. For example:

```
Subject: AW: [MLM-tag] German reply subject
```

can be transformed to:

```
Subject: Re: [MLM-tag] German reply subject
```

Therefore, if the field is signed, it is clever to save a copy of it as Original-Subject:.

3.1.2. From

From: rewriting is necessary for DMARC. That way, the MLM domain becomes the primary identifier of a message, in the DMARC sense. It is often achieved by transforming a field like this:

```
From: Original User <user@example.com>
```

into one like the following:

```
From: Original User via MLM <MLM.post@list.example>
```

MLMs can save the original value of From: in a variety of places, including Reply-To:, Cc:, X-Original-From:. When the original value is known, the transformation is revertible.

Author's domain submission agents can also provide a copy of From: in one of the fields Author: [RFC9057] and Original-From: [RFC5703]. Besides providing revertibility, signing that field signals participation and explicitly asks for feedback reports.

3.2. Body Transformations

We only consider footer addition. It is often performed in one of three ways, according to the format of the original message.

Single-part plain text
: When the original message is not structured, a footer can be appended at the end of the original text. See example in Appendix A.1

Multipart added
: The footer stands in its own MIME entity, which is appended as the last part of an original multipart/mixed structure. See example in Appendix A.2

Multipart wrapped
: The footer stands in the second entity of a new multipart/mixed MIME structure whose first entity consists of the original body. See example in Appendix A.3

The footer begins with a line consisting exclusively of underscore ("_", ASCII 95) characters, at least four of them. Alternatively, a footer can consist of the three characters "-- " (dash, dash, space), the Usenet signature convention (see for example Section 4.3 of [RFC3676]). For security reasons, the footer must belong to an

entity of Content-Type: text/plain in all cases. In addition, footers cannot exceed 10 lines of text, each shorter than 80 characters. If these restrictions are not met, the transformation cannot be reverted safely.

4. Outline of a Reverting Verifier

The algorithm described here is implemented in a mail filter [zdkimfilter]. The filter usually reads the input message twice - first pass, verify; last pass, write Authentication-Results and the rest of the message to follow. When enabling MLM transformation reversion, there can be a retry pass in between those two. The result is yielded during the SMTP dialogue with no noticeable delay. Implementing reversion changed the software from 22730 lines of C code to 26762. The bulk of such ~18% increase is due to the addition of encoding conversion functions. Changes involve both verifying and signing functions (see Section 5.1 for the latter).

While reading the header in the first pass, the verifier looks for specific fields:

- *From:
- *Author:
- *Original-From:
- *X-Original-From:
- *Reply-To:
- *Cc:

These are candidates to the original mailbox. Note that Reply-To: and Cc: may contain multiple mailboxes.

The verifier also collects the Subject: and any field named Original-* that the original signer might have set to ease the reversion. On reaching the end of the header, during the first pass, the verifier sorts the candidate original mailboxes according to the display name, which MLMs try and keep unaltered. The best candidate is then added to the collected set of Original-* fields. If the Subject: begins with a tag, its version without tag is added to that set as well, unless one is there already.

Next, before reading the body, the verifier looks for prospect signatures; that is, signatures whose "d=" domain is not aligned with SPF credentials ([RFC7208]), List-Post: ([RFC4201]), Sender:, or the rewritten From: (if deemed to have been rewritten). If any

such signature exist, along with MLM or other signatures, then the verifier enables parsing the body to look for a footer.

Reversing verifiers also have to watch out for idiosyncrasies used to mask DKIM signatures. For example, a MLM introduced a header field named X-Mailman-Original-DKIM-Signature, because some receivers took the habit to downgrade messages with failed signatures, despite [RFC6376] recommendation to consider an unauthenticated message regardless of whether or not it looks like it was signed. For authentication purposes, the first 19 characters of that field can be discarded.

Body parsing is done in parallel with body canonicalization during the first pass. For multipart, track top level entities. Set transformation type to "wrapped" if there are exactly two entities, "added" otherwise. However, some lists, perhaps out of misconfiguration, insert an empty attachment before the one containing the footer. As it is unlikely that a mail client sends an empty attachment, heuristically it may be preferable to just not count it. For single-part, body parsing must avail of encoding conversions as needed. Assume identity encoding, 7bit or 8bit, unless otherwise directed by an Original-Content-Transfer-Encoding: field.

At the end of the first pass, the verifier knows how prospect signatures did. Let's recall that DKIM signature verification results from two independent operations, steps 3 and 4 in Section 6.1.3 of [RFC6376]. The signature in the "b=" tag depends on the header, while the body hash in the "bh=" tag depends on the body:

* If the signature "b=" did not verify and the set of Original-* fields is not empty, then it is worth to try and re-canonicalize the header using the values in the set of Original-* fields.

* If the body hash "bh=" did not match and a footer was found, then it is worth to try and re-canonicalize the body excluding the footer.

None, one, or both of the above operations are performed in the retry pass.

On writing Authentication-Results, if a prospect signature verifies after replacing the From: field, the verifier writes a prominent, well documented "reason" in the relevant resinfo stanza (Section 2.2 of [RFC7601]). For example:

```
Authentication-Results: example.com;
  spf=pass smtp.mailfrom=list.example;
  dkim=pass reason="transformed" header.d=example.org;
  dkim=pass (whitelisted) header.d=list.example;
  dmarc=pass header.from=example.org;
```

That way, reversion elements can be easily recognized and parsed by downstream agents.

5. Actors Roles and Compliance

5.1. Original Signer

Signers who wish their users to be able to participate to mailing lists can adopt rules apt to ease MLM transformations reversion. A sender might abide by the following rules for all outgoing mail, or, if it had some idea which recipients are MLMs, could apply the rules only to mail to those recipients.

A first rule is the addition of an Author: header field with a value identical to the one signed in From:. Author: is defined for exactly this purpose in [RFC9057]. Original-From: can also be used, by analogy with other Original-* fields. It is defined in [RFC5703] in the context of Sieve Email Filtering.

If Author: is also signed by the author's domain, a reverting verifier should send DMARC feedback reports also to the original signer, even though From: was rewritten.

Note that [RFC7960] suggests that ReSenders can add an Original-From: too. Likewise, [RFC9057] suggests that Author: can be added by Mediators.

Other generic rules to ease reversion are as follows:

- DKIM signatures must deploy the "relaxed" canonicalization, at least for the header, since MLMs may reflow header fields.

- The quoted-printable encoding must not be used for the body of single-part text/plain messages, as it is impossible to guess original soft line breaks after re-encoding. Base64 is much more robust.

- Single-part text/plain messages encoded as base64 must follow a constant column width of 76 characters. The encoding must be advertised by adding a new header field as follows:

```
Original-Content-Transfer-Encoding: base64
```

*If the original Subject: begins with a tag (not Re: followed by a tag), its value must be copied to an Original-Subject: header field. The latter field is also defined by [RFC5703], and the same usage considerations hold.

*Content-Type: and Content-Transfer-Encoding: are fields related to the data form. Section 5.4.1 of [RFC6376] does not recommend to sign them. Mailers often rewrite them, so they must not be signed if signature robustness is a concern. If signed, their Original- counterpart should be set too.

*When signing Cc: or Reply-To:, add their Original- counterparts to the header, as MLMs are likely to change them, especially if they have multiple mailboxes.

Original-: fields with an empty value stand for non-existing counterparts.

Except as noted above for Author:, Original- fields need not be signed. If original signatures can be recovered, that suffices; otherwise, the unverified signature is irrelevant.

5.2. MLM

Participating MLMs must not operate transformations other than those listed in Section 3. Since DKIM is MIME-agnostic, attention must be paid to preserve the exact preamble and epilogue of the original MIME structure.

MLMs should apply their own DKIM signature.

It is recommended that MLMs insert a mailbox entry to Reply-To: or Cc: in order to ease off-list replies as well as to allow transformation reversion.

MLMs which collect posts from other MLMs must avoid to add their own footer and subject tag. Transformation reversion cannot be stacked. A second-level MLM can modify or replace the content of previous transformations. Attention must be paid to not exceed tag and footer length limits.

5.3. Verifier

Attempts to verify original signatures can be done as outlined in Section 4. The reversion must not alter the messages signed and distributed by MLMs, except for adding an Authentication-Results: header field, and possibly an Author: or an Original-From: field.

If an original signature with rewritten From: is recovered, the verifier must make sure that the original value of From: is written out in a field agreed upon by downstream agents, typically Original-From:. An MDA downstream may combine the Authentication-Results: with that field to restore the original value of From:. This is the only recommended modification to the distributed message. It must be done after any dot-forward processing, so that external verifiers receive the message as distributed by the MLM, and can revert transformations by themselves.

If the Author: field is found and if it was included in the h= tag of the original signature, the corresponding DMARC record may be looked up and its "rua=" and "ruf=" tags considered for feedback reports, whatever the result. However, if applying DMARC policies is considered, it is the From: field which rules, not the Author:, Original-From:, Sender:, nor any other mailbox domain.

6. Security Considerations

Rewriting the From: header field is a treacherous modification to messages. It fosters the belief that the display name of a mailbox is more true than the angle address. A belief further consented by the tendency to not even display the latter. Bad actors take advantage of this belief by displaying the names of trusted institutions paired with trash email addresses hidden between angle brackets. That trick defeats DMARC's purpose.

It is out of this document's scope to suggest how mail user agents (MUAs) could counter phishing by highlighting security indicators (for the extent that indicators can actually help preventing phishing attacks). Let's just note that MUAs have to cope with MLM and phishing alike, which makes it hard to devise a pattern to tell apart one from the other without getting involved with the reputation of the specific domains.

By safely restoring munged From: to the original value, that contrast is eliminated. Then, perhaps, deceptive mailboxes might become amenable to some kind of efficient indication.

Of course, MLM role can be played by miscreants as well. However, replaying a signed message, even with revertible transformations, has more limits than forging scam messages anew. Therefore, the risk introduced by easing transformation reversion is considerably lower than that of not signing, or of keeping DMARC policy at "none".

An unlikely risk is that of a fake MLM sending messages with Author: signed by a broken signature in order to trick a reverting verifier into sending false feedback reports.

Compared with the use of "l=" tag (Section 8.2 of [RFC6376]), the fact that footers are written in plain text removes the main security objection about footer additions. Namely, footers cannot completely replace the original content in the end recipient's eyes by exploiting lax HTML parsing in the MUA.

Still, a footer can contain dangerous URLs and deceiving text. That possibility has to be countered by usual mail filtering and savvy behavior.

7. IANA Considerations

IANA maintains the "Message Header" registry with several subregistries. IANA is asked to make the assignments set out in the following section.

7.1. Provisional Message Header Field Names

IANA is asked to create new entries in the "Provisional Message Header Field Names" registry as follows.

Header Field Name	Template	Protocol	Status	Reference
Original-Content-Transfer-Encoding		mail	standard	this I-D
Original-Reply-To		mail	standard	this I-D
Original-Cc		mail	standard	this I-D

Table 1

8. Experimental Goals

Mailing lists are a tool of the trade in a number of communities, including IETF. In order to preserve the confidence in it as is provided by the end-to-end nature of mail identifiers also in the face of DMARC disruption, the feedback this experiment seeks can be sketched in the following goals:

*Are signers or MUA willing to add the Author: field?

*How much change is needed to adapt more DKIM verifiers to revert the restricted set of transformations described here so as to verify original signatures and restore the original value of From:?

*Alternatively, a receiver could trust an Authenticated Received Chain (ARC) [RFC8617] and use the value of Author: to restore the original value of From:. There are some outstanding loose points in doing so, but how do these two possibilities compare? What is the security vs. ease of setup tradeoff?

*What are the incentives to make the changes?

9. References

9.1. Normative References

[RFC2045] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, DOI 10.17487/RFC2045, November 1996, <https://www.rfc-editor.org/info/rfc2045>.

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

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

[RFC6376] Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed., "DomainKeys Identified Mail (DKIM) Signatures", STD 76, RFC 6376, DOI 10.17487/RFC6376, September 2011, <https://www.rfc-editor.org/info/rfc6376>.

[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/info/rfc7489>.

[RFC9057] Crocker, D., "Email Author Header Field", RFC 9057, DOI 10.17487/RFC9057, June 2021, <https://www.rfc-editor.org/info/rfc9057>.

9.2. Informative References

[RFC3676] Gellens, R., "The Text/Plain Format and DelSp Parameters", RFC 3676, DOI 10.17487/RFC3676, February 2004, <https://www.rfc-editor.org/info/rfc3676>.

[RFC4201] Kompella, K., Rekhter, Y., and L. Berger, "Link Bundling in MPLS Traffic Engineering (TE)", RFC 4201, DOI 10.17487/RFC4201, October 2005, <https://www.rfc-editor.org/info/rfc4201>.

[RFC5703] Hansen, T. and C. Daboo, "Sieve Email Filtering: MIME Part Tests, Iteration, Extraction, Replacement, and Enclosure", RFC 5703, DOI 10.17487/RFC5703, October 2009, <https://www.rfc-editor.org/info/rfc5703>.

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

[RFC6377] Kucherawy, M., "DomainKeys Identified Mail (DKIM) and Mailing Lists", BCP 167, RFC 6377, DOI 10.17487/RFC6377, September 2011, <https://www.rfc-editor.org/info/rfc6377>.

[RFC7208] Kitterman, S., "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1", RFC 7208, DOI 10.17487/RFC7208, April 2014, <https://www.rfc-editor.org/info/rfc7208>.

[RFC7601] Kucherawy, M., "Message Header Field for Indicating Message Authentication Status", RFC 7601, DOI 10.17487/RFC7601, August 2015, <https://www.rfc-editor.org/info/rfc7601>.

[RFC7960] Martin, F., Ed., Lear, E., Ed., Draegen, T., Ed., Zwicky, E., Ed., and K. Andersen, Ed., "Interoperability Issues between Domain-based Message Authentication, Reporting, and Conformance (DMARC) and Indirect Email Flows", RFC 7960, DOI 10.17487/RFC7960, September 2016, <https://www.rfc-editor.org/info/rfc7960>.

[RFC8617] Andersen, K., Long, B., Ed., Blank, S., Ed., and M. Kucherawy, Ed., "The Authenticated Received Chain (ARC) Protocol", RFC 8617, DOI 10.17487/RFC8617, July 2019, <https://www.rfc-editor.org/info/rfc8617>.

[zdkimfilter] "zdkimfilter", <https://www.tana.it/sw/zdkimfilter/>.

Appendix A. Examples

In the examples that follow, the first character of each wrapped line of DKIM-Signature: fields should be a TAB. For editorial reasons, it is rendered as four spaces. While visually there is little difference, those signatures won't verify unless replacing them with a TAB.

To verify the examples, public keys can be set as follows:

```
s._domainkey.example.com IN TXT ( "v=DKIM1; g=*; k=rsa; "
"p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCqlye7m5zLLXoIpBp2OO05LNMqK"
"u0zKowoHOpyRpviOVqOaNCk5uZ+wY00JwrKbt5u1G1ghuXsFkFkl0h00LBurz7ivyZH"
"3LohSWOZ8okgR+8kuGu9GHtQ+MqgRd16tlCF8PlWS2kGaBQKua1zk+ZCDwFy82Uo5G2"
"1nu/+Nn2sUwIDAQAB" )

s._domainkey.lists.example IN TXT ( "v=DKIM1; k=rsa; "
"p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDgnLb2TZ6KECBMBo9ZLqDFt4ZBz"
"NHFrgBj/LVJVFU8IQP8uH4G8Pj0mEHRo1qpf0vuFI2HVpe/3NhzkT4Ay/1ZIIsxY754"
"f2thlhBvKh4AAgZFmzRvA3aZs6Tb/ERmD+a51liEMFaTOmY4mWeLi9wOM51usQ9Q65i"
"8IP/vjHM3rQIDAQAB" )
```

A.1. Single-part plain text

Base64 encoding has to be decoded in order to locate the footer. The original encoding was text/plain, this can be inferred by the verifier from the absence of an Original-Content-Transfer-Encoding: field. The original body hash will match after decoding and removing the footer. Note that an "l=" tag couldn't have done the trick in this case.

```
Received: from lists.example by subscriber.example.org with ESMTP
DKIM-Signature: v=1; a=rsa-sha256; c=simple/simple; d=lists.example; s=s;
    t=1603901305; bh=MjC5ikx26j8beyDJiz7Rk/4W+ppdGOmqh6koz0gLa8o=;
    h=Date:From:To:Subject;
    b=PNIYHGd7aytHEvew44WRpSfl4Py3c/9mKjovvQ1ps/xdpkl1/z+gWeu8e8ZmR7gdE
     iT2TsJ7ni3Lfp5oUpGCko5MvCoqcKX7Zmq3CmXTxRTwwvVZrAp/ir8UTvG+rJFnyEZ
     Yi3dSTX4rKe2LotyLkqcs+/uXaWEADbqcBp/9iHo=
Received: from mail.example.com by lists.example with ESMTP
DKIM-Signature: v=1; a=rsa-sha256; c=simple/simple; d=example.com; s=s;
    t=1603889142; bh=hrDXocZNPy1+eUFYIk1PVRKa6mUMb8+ql9CFNABacww=;
    h=Date:From:To:Subject;
    b=YFLwvvW5bGbE5HpJwBM1JoL1F9b8AxdVFlwE/vOkL0p/pPpr7g9KnPXqwoEXZgFI0
     /kkTHK/Afy4gaWZQfwDZ77LuxYSMFjwpNorSc0YEGzHYzLCN7rL1e+xE7B7kOCThiq
     ebaMdcaHeZF6QUmWcUkEj8LVkxrvWi+bTzd3RnaA=
Original-From: Author <user@example.com>
Received: from mua.example.com by mail.example.com with ESMTPA
Message-ID: <123456@author.example>
Date: Mon, 28 Oct 2020 13:12:55 +0100
From: Author <user@example.com>
MIME-Version: 1.0
To: MLM@lists.example
Subject: [example] Check simple MLM message
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: base64

VGhpcyBpcyBhIHBsYWluIHRleHQgbWVzc2FnZSBzdWJtaXR0ZWQgdG8gYSBtYWlsaW5nIGxpc3Qu
ClRoZSBtYWlsaW5nIGxpc3QgaXMgZXhwZWN0ZWQgdG8gYWRkIGEgZm9vdGVyIGFuZCBhIHN1Ympl
Y3QgdGFnLgoKQmVzdApBdXRob3IKCl9fX19fX19fX19fX19fX19fX19fX19fX19fX19fX19f
X19fX18KdGhpcyBtZXNzYWdlIHdhcyBtb2RpZmllZCBieSBNTE0gZXhhbXBsZQphZGRpbmcgdGhp
cyBmb290ZXIgYW5kIHRoZSBzdWJqZWN0IHRhZwoobm90ZSB0aGF0IGw9IGlzIG5vdCBzZXQpCg==
```

A.2. Multipart added

When the original message has a MIME structure, MLMs can append an entity.

```
Received: from lists.example by subscriber.example.org with ESMTP
DKIM-Signature: v=1; a=rsa-sha256; c=simple/simple; d=lists.example; s=s;
    t=1603974193; bh=sEPYSlJlh90leqy5+63oPn1iU+9P684R92cZHXa9ENw=;
    h=Date:From:To:Subject;
    b=fTSAMcaEatofQCuAeUhlTXmVl5j9bPbwWgc84NWtoSt5zT+SSNp37DTzhYIGHozEk
     bpldArGQ+GygJE1b2witi6NctBd1O/xsUwDcJQxDXkF63QlCcalbKWypHZOhRqncUQ
     zgUzdcuYgqTYMJ0NoTP8fqu0HdgmjD2LJXjV3pVI=
Old-Authentication-Results: lists.example;
  dkim=pass header.d=example.com
Received: from mail.example.com by lists.example with ESMTP
DKIM-Signature: v=1; a=rsa-sha256; c=simple/simple; d=example.com; s=s;
    t=1603973996; bh=eWqyE53pjRVCFGyHY1zGQTkCEvucN1vNN4cTcWk90WU=;
    h=Date:From:To:Subject;
    b=LGP1M3IX6XORfLs8HRLCFOcymzsPn+8+ljgQlmeNlCC/2Cl1+aBDCIEnzWI0pceCb
     zg32vFfEeryvRDHB1L1K4rrKCEznvO0J3p1xkUPEWpSpzxUGw+PK9KA9ePZ5qdz7cI
     /hXf7zjebznNdDQJnxajf7QHnx1tXmxijsJ1jiGQ=
Old-Authentication-Results: example.com; auth=pass (details omitted)
Original-From: Author <user@example.com>
Received: from mua.example.com by mail.example.com with ESMTPA
Message-ID: <123456@author.example>
Date: Mon, 28 Oct 2020 13:12:55 +0100
From: Author via MLM <MLM@lists.example>
MIME-Version: 1.0
To: MLM@lists.example
Subject: [example] Check simple MLM message
Content-Type: multipart/mixed; boundary=original-boundary

Original preamble must be preserved!

--original-boundary
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit

This is a plain text message submitted to a mailing list.
The mailing list is expected to add a footer and a subject tag.

Best
Author

--original-boundary
Content-Type: image/png
Content-Transfer-Encoding: base64

iVBORw0KGgoAAAANSUhEUgAAAAYAAAAGCAYAAADgzO9IAAAABHNCSVQICAgIfAhkiAAAAAlwSFlz
AAAHKgAAByoB49HU1wAAABl0RVh0U29mdHdhcmUAd3d3Lmlua3NjYXBlLm9yZ5vuPBoAAAB+SURB
VAiZNcGxDYUgAEXRhxTMYWLFVlDTOAUjOIEzWDqEC1igCQ0LSLi/+ueotUZKieu6uO+bdV2ptaLz
PDHGsG0b+74jieM40Pd91Fr5K6UAMC3LImutxhgaY8g5p3meNcUYFULQ+756nkchBMUYpd47OWe8
93jvyTnTe+cHXqRZbKSV4EoAAAAASUVORK5CYII=
```

```
--original-boundary
Content-Tyep: text/plain

_____________________________________________
this message was modified by MLM example
adding this footer and the subject tag
(note that l= cannot work in this case)

--original-boundary--
```

A.3. Multipart wrapped

When the original body is multipart/alternative, MLMs have to wrap the whole body into the first entity of a multipart/mixed structure. Indeed, appending an entity to a multipart/alternative would result in it either hiding or being hidden by the existing ones.

```
Received: from lists.example by subscriber.example.org with ESMTP
DKIM-Signature: v=1; a=rsa-sha256; c=simple/simple; d=lists.example; s=s;
    t=1603962061; bh=n4/RahgnfVg7htgJtCr7TwEW4eKA1O5oiNaQFA5HU+A=;
    h=Date:From:To:Subject;
    b=RJlq/Fu40AC1hdJfljd+KPU69Vq2M7capbGQyEMhDWvaN7xDPJdXotwnTwiz91iZY
     5W3ITY7YXKHsWweLxu1Rph3ST3bbYQ1cifztpmtu4VPifBkm9MAe7OMDLHhk5ua9YL
     VzJOsXieiIw5a8JhOsr6F/05/K05kNiEXvuLgKd8=
Old-Authentication-Results: lists.example;
  dkim=pass header.d=example.com
Received: from mail.example.com by lists.example with ESMTP
DKIM-Signature: v=1; a=rsa-sha256; c=simple/simple; d=example.com; s=s;
    t=1603961679; bh=XiCPbOV1vcu2Q2TyEUOuT4SMun2AjYj/Va6KRPa1lv0=;
    h=Date:From:To:Subject;
    b=gvM5grV2dbtinFMLcExv+gMATILzY+c8RY7QPVBJSFohH5HMgOLwrgSH8uwOcZxq0
     FoXtBcHnukonqo97l8nY0faHi0Dp0LAmqn9e4ijwXw9IWwhFuUiCwICRaLEzrNUVBN
     TWtzkQKnHpEXnPGBD7Q9f924mBe+eZsDyRc41ZvQ=
Old-Authentication-Results: example.com; auth=pass (details omitted)
Original-From: Author <user@example.com>
Received: from mua.example.com by mail.example.com with ESMTPA
Message-ID: <123456@author.example>
Date: Mon, 28 Oct 2020 13:12:55 +0100
From: Author via MLM <MLM@lists.example>
MIME-Version: 1.0
To: MLM@lists.example
Subject: [example] Check simple MLM message
Content-Type: multipart/mixed; boundary=MLM-boundary

This is the MLM preamble, not signed by Author.

--MLM-boundary
Content-Type: multipart/alternative; boundary=original-boundary

Original preamble must be preserved!

--original-boundary
Content-Type: text/plain;

This is a plain text message submitted to a mailing list.
The mailing list is expected to add a footer and a subject tag.

Best
Author

--original-boundary
Content-Type: text/html;

<p>This is a plain text message submitted to a mailing list.
The mailing list is expected to add a footer and a subject tag.

<p>Best<br>
```

Author

--original-boundary--

Original epilogue

--MLM-boundary
Content-Type: text/plain

---

this message was modified by MLM example
adding this footer and the subject tag
(note that l= is not set)

--MLM-boundary--

MLM epilogue

Author's Address

Alessandro Vesely
v. L. Anelli 13
20122 Milano MI
Italy

Email: vesely@tana.it