Network Working Group
Internet-Draft
Obsoletes: 4686 (if approved)
Intended status: Standards Track
Expires: 20 December 2025

B. Gondwana
Fastmail Pty Ltd

18 June 2025

A method for describing changes made to an email
draft-gondwana-dkim2-modification-alegbra-02

Abstract

This memo describes a method for describing the changes made to an email during common email modifications, for example those caused by mailing lists and forwarders.

While this is general enough to be used for any changes, it is anticipated that this method will normally be used for removing added data rather than large complex changes.

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 20 December 2025.

Copyright Notice

Table of Contents

1. Background and motivations

Currently, when an email is sent with a DKIM signature, the message can go through multiple forwarders and still be authenticated, however if a single change is made to a header which is covered by the signature, or to the body, then the signature no longer validates - and it's impossible for the receiver to know what was changed, or even if the entire message was replaced.

By producing a way to describe changes, the recipient can examine the sections which were changed and determine whether the change was malicious. Because each step signs its own changes in DKIM2, this also allows the recipient to identify exactly which intermediary introduced each change, and adjust their reputation accordingly.

2. Delta format - headers

For headers, the format is to completely replace all headers with a particular name. For example if you replace the subject and from address in an email, then you need to include the complete old headers for each of those:

Header: "DKIM2-Delta-Header:"

Command	Input
i	DKIM2 matching header number
b	replace headers with base64 octet value
t	replace headers with raw text characters value

Table 1

Example for a message which has had Subject and From replaced, and Reply-To added.

```
From: brong@fastmailteam.com.dmarc.fail
To: dkim2@lists.ietf.org
Reply-To: dkim2@lists.ietf.org
DKIM2-Delta-Header: i=3;
 t=Subject:A replacement for DKIM;
 b=From:YnJvbmdAZmFzdG1haWx0ZWFtLmNvbQo=;
 t=Reply-To
```

Notice that "Reply-To" has no colon, and hence is an instruction to remove any "Reply-To" headers. All headers are case insignificant for removal, and SHOULD be inserted with the case given in the header when being added back.

3. Delta format - body

This difference format for the body was originally going to be an octet-based change format, however this is incompatible with "relaxed" signature checks as line ending normalisation could change the octet lengths, so this format was changed to be line based.

Since the transport for the delta is a 7-bit mime header, this format has been made simple and human readable. It is a simple program describing ranges of data to copy from the output to recreate the input.

Header: "DKIM2-Delta-Body:"

Command	Input
i=n	DKIM2 matching header number
b=b64val	decode the value as base64 an insert the resulting octets as a line
c=a-b	insert the numbered lines from a to b inclusive (starting at 1)
t=value	insert the text of the value as a line
z=y	MUST be the only source; changes are not reversible via this mechanism

Table 2

Example:

DKIM2-Delta-Body: i=2; c=1-500; c=520-520

Example - a URL was substituted in the content of the body (complex, but still easily doable!)

```
DKIM2-Delta-Body: i=3;
 c=1-500;
 b=PGEgaHJlZj0iaHR0cHM6Ly93d3cuZXhhbXBsZS5jb20iPkV4YW1wbGU8L2E+Cg==;
 c=501-702
```

The decision whether to use ’b’ or ’t’ is up to the system creating the diff, however ’t’ has a limited set of characters that are safe to use in headers.

Likewise, it is expected that ’c’ will normally be used to copy lines directly from the new message, however in cases where a message needs to transit 7 bits systems cleanly, the email modifier may need to re-encode the octets of the original message, and this allows for doing so.

4. Signature coverage.

Each DKIM2 signature implicitly covers all DKIM2-Delta-Body and DKIM2-Delta-Header headers with an i=N value for the same and lower N values as the i= on the DKIM2 header.

5. Iterative application

To get back to the original message and confirm that it was unchanged, it is necessary to apply this algorith iteratively.

For example if you receive a message at i=7 for which there is a modification to the headers at i=5 and a modification to both headers and body at i=3, to recreate the original message you would first apply the header changes from i=5, then apply the header and body changes for i=3. If this doesn't create a message which validates with the initial i=1 signature, then some hop has corrupted the message, and you can check every single DKIM signature in reverse to find the first one where the message no longer validates.

6. Security

TBA

7. IANA Considerations

TBA

8. Informative References

[RFC2046] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", RFC 2046, DOI 10.17487/RFC2046, November 1996, <https://www.rfc-editor.org/rfc/rfc2046>.

[RFC3284] Korn, D., MacDonald, J., Mogul, J., and K. Vo, "The VCDIFF Generic Differencing and Compression Data Format", RFC 3284, DOI 10.17487/RFC3284, June 2002, <https://www.rfc-editor.org/rfc/rfc3284>.

Appendix A. Changes from Earlier Versions

A.1. draft-gondwana-dkim2-modification-algebra-02

* change to using line numbers rather than octet offsets
* remove d= base64 decoding capability
* for multiple lines; require a separate b= or t= for each line

A.2. draft-gondwana-dkim2-modification-algebra-01

* rename 'DKIM2-Diff' headers to 'DKIM2-Delta'

* add ’z=y’ option to DKIM2-Delta-Body for "complete replacement"

* add d= base64 decoding option to DKIM2-Delta-Body

A.3. draft-gondwana-dkim2-modification-algebra-00

* original version

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

Author’s Address

Bron Gondwana
Fastmail Pty Ltd
Level 2, 114 William Street
3000
Australia
Phone: +61 457 416 436
Email: brong@fastmailteam.com