Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 4 September 2025

A. Brotman
Comcast, Inc

3 March 2025

Email Feedback Reports for DKIM Signers
draft-brotman-dkim-fbl-04

Abstract

Mechanism to discover a destination used to deliver user-supplied FBL reports to an original DKIM signer or other responsible parties. This allows the reporting entity to deliver reports for each party which has affixed a validating DKIM signature. The discovery is made via DNS and the record is constructed using items within the DKIM signature in the message.

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 4 September 2025.

Table of Contents

1. Introduction

Historically, Feedback Loops (FBL), typically comprised of False Positive (FP) and False Negative (FN) reports, have allowed users the ability to inform their Mailbox Provider (MBP) that they disagree with a message’s placement in the Inbox or Spam folder. In some situations, an MBP may then forward that feedback directly, or via an intermediary, to the original source system of that message. Traditionally, this source system identified via a registration system, typically tying a set of IPs or DKIM-based domains to a specific reporting location.

By allowing reporters to discover the destination and reporting preferences on their own, this could reduce friction getting FBLs to the original DKIM signer(s).

This document is meant to enable a method by which a MBP can discover how to report feedback in the form of an FBL. This is *not* meant to demonstrate how a MBP can provide feedback about DKIM-related issues.

2. Discovery using DNS

There are alternative approaches for discovering the feedback information proposed. This document describes a method for using DNS to discover a feedback address by utilizing the DKIM signature(s) within a message itself.

The advantage of the DNS approach is that it can be changed after messages are delivered, allowing for old reports to be processed after migrating to a new report processing provider. It also avoids common problems with modifying headers of messages that are already signed by another DKIM signature.

Email service providers and intermediaries, which have a shared responsibility with an upstream sender, will commonly add their own DKIM signatures to the messages, thus resulting in the message having two signatures in different DKIM d= domains. Dual-signed messages will result in feedback going to the location specified in the DNS for both domains. Thus there is no reason to modify any message headers and potentially break the original DKIM signature.

3. DNS Record Location

The record will combine a label with the "d" value from the DKIM signature in the message being sent, optionally using a DNS wildcard (* character). Such as the case where "d=example.org", the record would be located at:

_feedback._domainkey.example.org

or

*._feedback._domainkey.example.org

If the reporting destination needs to be different for individual DKIM selectors, each selector will need a DNS record with a value combined with a label with the "s=" value from the DKIM signature in the message being sent. Such as the case where "d=example.org", and "s=contact", for example:

contact._feedback._domainkey.example.org

By including the selector, this allows a domain to be able to segment the feedback to various report processing providers, but a wildcard can no longer be used as a catch-all and an individual record must be created for each selector in use. DKIM selectors are not supposed to be used for identification purposes, and they should change frequently to facilitate key rotation.

The need for selector level feedback still needs to be assessed.

All domain owners that want to ensure they receive all feedback should, at a minimum, publish a record at the following location as a catch-all:

_feedback._domainkey.example.org

The DNS entry will contain a TXT record described below.

4. DNS Record Format

The DNS record MUST contain the information necessary for a report generator to send the feedback to the proper location.

v: A string identifying the record. The value must be "DKIMRFBLv1"

ra: An address destination for reports. The address should match the format defined in [RFC5321]. If there is a "rfr" entry, the "ra" may be omitted. If there is more than one target address, the entries must be separated by a comma (","). The destination MUST use a classification of "mailto" or "https", indicating the transfer methods supported by the DKIM signer.

rfr: An optional field to refer the report generator(s) to another DNS entry.

c: Content flag. If set to 'n', the reporting entity SHOULD remove all content beyond the headers of the original message that is being reported. The default is "y".

h: The header by which the signer can identify the recipient, sender, and campaign. If a report generator is trying to create a minimalistic report, this would be the minimum amount of information to properly act on the report. This field is OPTIONAL, and MUST contain only one attribute.

hp: The header by which the signer can only identify the campaign. If present, the report generator may use the hp header instead of the h header if the recipient needs to remain private and there is no expectation of future sending to the recipient to be suppressed. This field is OPTIONAL, and MUST contain only one attribute.

f: Format requested by report receiver. Options are "arf" or "xarf". Default is "arf", and multiple values may be separated by a comma (,). If a report sender is unable to generate a report in a requested format, they SHOULD NOT send a report.

4.1. DKIM Requirements

If a sender utilizes the h or hp attributes in their DNS record, those fields MUST be covered by the DKIM signature that is requesting the report. If the header is not signed by the proper requestor (or not valid), the receiver SHOULD refuse to generate any reports for those related messages.

4.2. Examples

```
_feedback._domainkey.example.org TXT
"v=DKIMRFBLv1;ra=mailto:reporting@feedback.example.org"
(mailto:reporting@feedback.example.org")

contact._feedback._domainkey.example.org TXT
"v=DKIMRFBLv1;rfr=_feedback._domainkey.example.org"

contact._feedback._domainkey.example.org TXT
"v=DKIMRFBLv1;ra=mailto:fbl@example.org;rfr=_feedback._domainkey.exam
ple.org"
(mailto:fbl@example.org;rfr=_feedback._domainkey.example.org")

*._feedback._domainkey.example.org TXT
"v=DKIMRFBLv1;ra=mailto:other_fbl@example.org"
(mailto:other_fbl@example.org")

_feedback._domainkey.example.org TXT
"v=DKIMRFBLv1;c=n;ra=https://ra.example.org/
reports;h=SendingIdentifer" (https://ra.example.org/
reports;h=SendingIdentifer")

_feedback._domainkey.example.org TXT
"v=DKIMRFBLv1;ra=mailto:fbl@example.org;hp=Campaign-Id;c=n"
(mailto:fbl@example.org;hp=Campaign-Id;c=n")
```

_feedback.domainkey.sender.com TXT
"v=DKIMRFBLv1;ra=mailto:fbl@other.com;h=SendingIdentifier;hp=Capaign-Id;c=y;f=xarf" (mailto:fbl@other.com;h=SendingIdentifier;hp=Capaign-Id;c=y;f=xarf")

5. Report Contents

5.1. arf

When the report format is specified as "arf", the report contents should adhere to [RFC5965]

5.2. xarf

When the report format is chosen as "xarf" [XARF], the report generator should reference the materials below as to the format. XARF follows a JSON format and the format may change over time to match that specification.

The current format can be referenced:

https://github.com/abusix/xarf/blob/master/schemas/3/spam.schema.json (https://github.com/abusix/xarf/blob/master/schemas/3/spam.schema.json)

5.3. Aggregate FBL Reports

A reporting entity may desire to send only aggregate data for a given time period, and that report may not contain any content of the original messages. When this is the case, the reporter should utilize the hp field in the DNS declaration to be used as the value by which the sender will be able to recognize the message stream.

The hp field MUST be signed by the corresponding DKIM signature, and that signature must validate. As a message may be signed by multiple signatures, it’s possible that there could be multiple headers match an hp definition.

If the DNS declaration does not include an hp field, or the signature is valid, a reporting entity MUST NOT generate a report for the related messages.

5.3.1. Report Format

NOTE: This could be created as an XARF, TBD

```
<feedback>
<report_metadata>
<date_range>
<begin>15141231</begin>
<end>15152525</end>
<date_range>
<report_id>20231212-8gKW3RA34VWa3ra</report_id>
<selector>dkim_sel</selector>
<domain>dkim_domain</domain>
<feedback_header>HeaderName</feedback_header>
<header_contents>123:c21vRA3-V3A</header_contents>
</report_metadata>
<record>
<row>
<source_ip>1.2.3.4</source_ip>
<fn_complaints>3</fn_complaints>
</row>
</record>
</feedback>
```

6. Content Flag

Some DKIM signers may prefer that they only receive headers from a reporter. The reporter SHOULD attempt to adhere to those wishes of the signer. In a situation where c=n and h has a value, the report generator would send a report with only that single header. if the 'hp' tag has a value then the report generator MAY use that value instead of the 'h' tag if the recipient's privacy needs to be preserved at the expense of future sending possibly not being suppressed to that address.

7. Delivery Methods

Reports MUST be sent to the address specified by the "ra" tag.

7.1. mailto

Refer to [RFC5965]

7.2. https

A DKIM signer may specify that they wish to receive reports via HTTPS. When doing so, the reporter should continue to use the format specifed by the rest of the declaration.

NOTE: Consider if HTTPS should be supported, based on historical usage patterns for other similar mechanisms

The report generator SHOULD follow redirects.

The HTTPS method MUST be POST.

HTTPS GET requests to the URL MUST provide easy to follow instructions for users to report complaints.

The report generator SHOULD NOT remove parameters from the URL before submitting the report unless the 'hp' tag is specified. If the 'hp' tag is specified then the parameters can be removed if the report generator needs to preserve the privacy of the recipient at the expense of the report not causing suppressed sending to that recipient in the future.

DNS record

v=DKIMRFBLv1;c=n;ra=https://ra.example.org/dkim-fbl?track=xzy;h=Message-Id;hp=Feedback-Id (https://ra.example.org/dkim-fbl?track=xzy;h=Message-Id;hp=Feedback-Id)

Header in Email

DKIM-FBL: https://ra.example.com/reports (https://ra.example.com/reports) Message-Id: opaque@example.com Feedback-Id: opaque

Resulting POST request

POST /dkim-fbl?optional=opaquePart HTTP/1.1 Host: ra.example.com Content-Type: application/x-www-form-urlencoded Feedback-Type: abuse Content-Length: 26

... NEED examples of each: arf and xarf to provide the 'h' or 'hp'

7.2.1. https Feedback-Type Header

A reporter MAY include a HTTP header that denotes which report type is being delivered. If used, the header MUST be titled "Feedback-Type", and adhere to the definition referenced in [RFC5965] section 7.3 or the associated IANA declarations. If this header is absent, the Feedback-Type MUST be considered "abuse".

8. Verifying External Destinations

In order to limit the possibility of misdirected reports, if the receiving entity domain does not align to the d= of the DKIM signature, there must be a DNS record to verify the external destination.

Domain alignment is determined by the logic defined by [DMARCbis]. Domain alignment applies to domain of the email address in the 'rua' tag if the 'f' tag is 'arf' or 'xarf'. Domain alignment applies to the domain defined in the URI of the header referenced by the 'rua' tag if the 'f' tag is 'https'

Consider the record:

foo._feedback._domainkey.example.org TXT
"v=DKIMRFBLv1;ra=mailto:reporting@othersite.com"
(mailto:reporting@othersite.com")

In order for "othersite.com" to receive reports for this DKIM signature, a record must exist at specified location, and contain a specified value.

1. Using the domain of the destination
2. Prepend "_report._feedback"
3. Prepend the values from d= and s= from the original signature.
4. Ensure the value is set to "v=DKIMRFBLv1"

foo.example.org._report._feedback.othersite.com TXT "v=DKIMRFBLv1"

If the feedback receiver is comfortable with receiving feedback for all selectors within a domain, then they may omit the s= value from the DNS record location. The record would be named:

example.org._report._feedback.othersite.com TXT "v=DKIMRFBLv1"

9. Security Considerations

9.1. Feedback to Malicious Senders

There is some concern that a MBP may provide some advantage or useful information to a malicious entity by providing them with FBL data. Each MBP should use their own judgement when deciding where to send reports. It is possible that an attacker could use this information to attempt to bypass anti-spam filters, or to validate a recipient at a given site.

9.2. Report Contents for ARF

Noting in [RFC5965] section 2.g, there should be enough information for most senders to process a complaint without the content of the message. While the c flag allows the report receiver to state that they do not wish to receive content, the report generator, as per [RFC5965] does not need to include that information, regardless of the flag settings.

10. Other Considerations

10.1. Supplying FP Reports

It is at the discretion of the report generator as to whether they supply False Positive reports, or aggregate information, to the report requester.

10.2. Site Requirements

A report generator may place some requirements on the sender in order to be eligible to receive reports. This could include something such as a DMARC policy requirements, TLS usage, or some level of reputation.

11. Contributors

12. Notes

13. Appendex

13.1. Samples

13.1.1. Sample message

DKIM-Signature: d=example.com;s=Selector1;h=From:To:Subject:Message-Id:Campaign-Id:Date From: "Sender" marketing@example.com (mailto:marketing@example.com) To: "Customer" recipient@example.net (mailto:recipient@example.net) Subject: SubjectHere Message-Id: awav4w4vaw.aw4473737bab.AWAe@sender (mailto:awav4w4vaw.aw4473737bab.AWAe@sender) Campaign-Id: 20240314a_Sender FBL-Message-Id: fgjm7Bbbse56b.Sender.recipient.example.net Date: March 24th, 2024 12:34.000UTC

Click here for stuff <EOM>

13.1.2. Sample DNS and Reports

13.1.2.1. Content-requested

DNS: v=DKIMRFBLv1;ra=mailto:fbl@example.com;c=y;f=arf (mailto:fbl@example.com;c=y;f=arf)

13.1.2.2. No Content Requested

DNS: v=DKIMRFBLv1;ra=mailto:fbl@example.com;c=n;h=Campaign-Id (mailto:fbl@example.com;c=n;h=Campaign-Id)

13.1.2.3. No Content, Summmary only

DNS: v=DKIMRFBLv1;ra=mailto:fbl@example.com;c=n;hp=FBL-Message-Id (mailto:fbl@example.com;c=n;hp=FBL-Message-Id)

Nothing should be delivered, as the FBL-Message-Id is not signed

14. References

[DMARCbis] https://datatracker.ietf.org/doc/draft-ietf-dmarc-dmarcbis/ (https://datatracker.ietf.org/doc/draft-ietf-dmarc-dmarcbis/)

15. Normative References

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

[RFC5965] Shafranovich, Y., Levine, J., and M. Kucherawy, "An Extensible Format for Email Feedback Reports", RFC 5965, DOI 10.17487/RFC5965, August 2010, <https://www.rfc-editor.org/info/rfc5965>.

Author’s Address

Alex Brotman
Comcast, Inc
Email: alex_brotman@comcast.com