DKIM Working Group
Internet-Draft
Intended status: BCP
Expires: November 11, 2011

M. Kucherawy
Cloudmark

May 10, 2011

DKIM And Mailing Lists
draft-ietf-dkim-mailinglists-10

Abstract

DomainKeys Identified Mail (DKIM) allows an administrative mail domain (ADMD) to assume some responsibility for a message. Based on deployment experience with DKIM, this Best Current Practices document provides guidance for the use of DKIM with scenarios that include Mailing List Managers (MLMs).

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 http://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 November 11, 2011.

Table of Contents

1. Introduction

DomainKeys Identified Mail [DKIM] allows an Administrative Mail Domain to take some responsibility for a [MAIL] message. Such responsibility can be taken by an author's organization, an operational relay (Mail Transfer Agent, or MTA) or one of their agents. Assertion of responsibility is made through a cryptographic signature. Message transit from author to recipient is through relays that typically make no substantive change to the message content and thus preserve the validity of the DKIM signature.

In contrast to relays, there are intermediaries, such as mailing list managers (MLMs), that actively take delivery of messages, re-format them, and re-post them, often invalidating DKIM signatures. The goal for this document is to explore the use of DKIM for scenarios that include intermediaries, and recommend Best Current Practices based on acquired experience. Questions that will be discussed include:

- Under what circumstances is it advisable for an author, or its organization, to apply DKIM to mail sent to mailing lists?
- What are the tradeoffs regarding having an MLM verify and use DKIM identifiers?
- What are the tradeoffs regarding having an MLM remove existing DKIM signatures prior to re-posting the message?
- What are the tradeoffs regarding having an MLM add its own DKIM signature?

These and others are open questions for which there may be no definitive answers. However, based on experience since the publication of the original version of [DKIM] and its gradual deployment, there are some views that are useful to consider and some recommended procedures.

In general there are, in relation to DKIM, two categories of MLMs: participating and non-participating. As each type has its own issues regarding DKIM-signed messages that are either handled or produced by them (or both), the types are discussed in separate sections.

The best general recommendation for dealing with MLMs is that the MLM or an MTA in the MLM's domain apply its own DKIM signature to each message it forwards, and for assessors on the receiving end to consider the MLM's domain signature in making their assessments. With the understanding that that is not always possible or practical, and the consideration that it might not always be sufficient, this document provides additional guidance.

1.1. Background

DKIM signatures permit an agent of the email architecture (see [EMAIL-ARCH]) to make a claim of responsibility for a message by affixing a validated domain-level identifier to the message as it passes through a relay. Although not the only possibility, this is most commonly done as a message passes through a boundary Mail Transport Agent (MTA) as it departs an Administrative Mail Domain (ADMD) across the open Internet.

A DKIM signature will fail to verify if a portion of the message covered by one of its hashes is altered. An MLM commonly alters messages to provide information specific to the mailing list for which it is providing service. Common modifications are enumerated and described in Section 3.3. However, note that MLMs vary widely in behaviour as well as often allowing subscribers to select individual behaviours. Further, the MTA might make changes that are independent of those applied by the MLM.

The DKIM signing specification deliberately rejects the notion of tying the signing domain (the "d=" tag in a DKIM signature) to any other identifier within a message; any ADMD that handles a message could sign it, regardless of its origin or author domain. In particular, DKIM does not define any meaning to the occurrence of a match between the content of a "d=" tag and the value of, for example, a domain name in the RFC5322.From field, nor is there any obvious degraded value to a signature where they do not match. Since any DKIM signature is merely an assertion of "some" responsibility by an ADMD, a DKIM signature added by an MLM has no more, nor less, meaning than a signature with any other "d=" value.

1.2. MLMs In Infrastructure

An MLM is an autonomous agent that takes delivery of a message and can re-post it as a new message, or construct a digest of it along with other messages to the members of the list (see [EMAIL-ARCH], Section 5.3). However, the fact that the RFC5322.From field of such a message (in the non-digest case) is typically the same as that of the original message, and that recipients perceive the message as "from" the original author rather than the MLM, creates confusion about responsibility and autonomy for the re-posted message. This has important implications for use of DKIM.

Section 3.3 describes some of the things MLMs commonly do that produce broken signatures, thus reducing the perceived value of DKIM.

Further, while there are published standards that are specific to MLM behaviour (e.g. [MAIL], [LIST-ID] and [LIST-URLS]), their adoption

has been spotty at best. Hence, efforts to specify the use of DKIM in the context of MLMs needs to be incremental and value-based.

Some MLM behaviours are well-established and their effects on DKIM signature validity can be argued as frustrating wider DKIM adoption. Still, those behaviors are not standards violations. Hence, the best approach for a BCP effort is to specify practices for all parties involved, defining the minimum changes possible to MLMs themselves.

A DKIM signature on a message is an expression of some responsibility for the message taken by the signing domain. An open issue that is addressed by this document is the ways a signature might be used by a recipient's evaluation module, after the message has gone through a mailing list and might or might not have been rendered invalid. The document also considers how invalidation might have happened.

Note that where in this document there is discussion of an MLM conducting validation of DKIM signatures or ADSP policies, the actual implementation could be one where the validation is done by the MTA or an agent attached to it, and the results of that work are relayed by a trusted channel not specified here. See [AUTH-RESULTS] for a discussion of this. This document does not favour any particular arrangement of these agents over another, but merely talks about the MLM itself doing the work as a matter of simplicity.

1.3. Feedback Loops And Other Bi-Lateral Agreements

A Feedback Loop (FBL) is a bi-lateral agreement between two parties to exchange reports of abuse. Typically, a sender registers with a receiving site to receive abuse reports from that site for mail coming from the sender.

An FBL reporting address (i.e., an address to which FBL reports are sent) is part of this bi-lateral registration. Some FBLs require DKIM use by the registrant.

See Section 6 for additional discussion.

FBLs tend to use the [ARF] or the [IODEF] formats.

1.4. Document Scope and Goals

This document provides discussion on the above issues, to improve the handling of possible interactions between DKIM and MLMs. In general, the preference is to impose changes to behaviour at the signer and verifier rather than at the MLM.

Wherever possible, the document's discussion of MLMs is conceptually

decoupled from MTAs despite the very tight integration that is sometimes observed in implementation. This is done to emphasize the functional independence of MLM services and responsibilities from those of an MTA.

Parts of this document explore possible changes to common practice by signers, verifiers and MLMs. The suggested enhancements are largely predictive in nature, taking into account the current email infrastructure, the facilities DKIM can provide as it gains wider deployment, and working group consensus. There is no substantial implementation history upon which these suggestions are based, and the efficacy, performance and security characteristics of them have not yet been fully explored.

2. Definitions

2.1. Key Words

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [KEYWORDS].

2.2. Messaging Terms

See [EMAIL-ARCH] for a general description of the current messaging architecture, and for definitions of various terms used in this document.

2.3. DKIM-Specific References

Readers are encouraged to become familiar with [DKIM] and [ADSP], which are core specification documents, as well as [DKIM-OVERVIEW] and [DKIM-DEPLOYMENT], which are DKIM's primary tutorial documents.

2.4. 'DKIM-Friendly'

The term "DKIM-Friendly" is used to describe an email intermediary that, when handling a message, makes no changes to that message which cause valid [DKIM] signatures present on the message on input to fail to verify on output.

Various features of MTAs and MLMs seen as helpful to users often have side effects that do render DKIM signatures unverifiable. These would not qualify for this label.

2.5. Message Streams

A "message stream" identifies a group of messages originating from within an ADMD that are distinct in intent, origin and/or use, and partitions them somehow (i.e., via changing the value in the "d=" tag value in the context of DKIM) so as to keep them associated to users yet distinct in terms of their evaluation and handling by verifiers or receivers.

A good example might be user mail generated by a company's employees, versus operational or transactional mail that comes from automated sources, versus marketing or sales campaigns. Each of these could have different security policies imposed against them, or there might be a desire to insulate one from the other (e.g., a marketing campaign that gets reported by many spam filters could cause the marketing stream's reputation to degrade without automatically

punishing the transactional or user streams).

3. Mailing Lists and DKIM

It is important to make some distinctions among different styles of intermediaries, their typical implementations, and the effects they have in a DKIM-aware environment.

3.1. Roles and Realities

Across DKIM activities, there are several key roles in the transit of a message. Most of these are defined in [EMAIL-ARCH], but are reviewed here for quick reference.

author: The agent that provided the content of the message being sent through the system. The author delivers that content to the originator in order to begin a message's journey to its intended final recipients. The author can be a human using an MUA (Mail User Agent) or a common system utility such as "cron", etc.

originator: The agent that accepts a message from the author, ensures it conforms to the relevant standards such as [MAIL], and then sends it toward its destination(s). This is often referred to as the Mail Submission Agent (MSA).

signer: Any agent that affixes one or more DKIM signature(s) to a message on its way toward its ultimate destination. There is typically a signer running at the MTA that sits between the author's ADMD and the general Internet. The originator and/or author might also be a signer.

verifier: Any agent that conducts DKIM signature analysis. One is typically running at the MTA that sits between the public Internet and the receiver's ADMD. Note that any agent that handles a signed message can conduct verification; this document only considers that action and its outcomes either at an MLM or at the receiver. Filtering decisions could be made by this agent based on verification results.

receiver: The agent that is the final transit relay for the message and performs final delivery to the recipient(s) of the message. Filtering decisions based on results made by the verifier could be applied by the receiver. The verifier and the receiver could be the same agent.

In the case of simple user-to-user mail, these roles are fairly straightforward. However, when one is sending mail to a list, which then gets relayed to all of that list's subscribers, the roles are often less clear to the general user as particular agents may hold multiple important but separable roles. The above definitions are

intended to enable more precise discussion of the mechanisms involved.

3.2. Types Of Mailing Lists

There are four common MLM implementation modes:

aliasing: An aliasing MLM (see Section 5.1 of [EMAIL-ARCH]) is one that makes no changes to the message itself as it redistributes; any modifications are constrained to changes to the [SMTP] envelope recipient list (RCPT commands) only. There are no changes to the message header or body at all, except for the addition of [MAIL] trace header fields. The output of such an MLM is considered to be a continuation of the author's original message transit. An example of such an MLM is an address that expands directly in the MTA, such as a list of local system administrators used for relaying operational or other internal-only messages. See also Section 3.9.2 of [SMTP].

resending: A resending MLM (see Sections 5.2 and 5.3 of [EMAIL-ARCH]) is one that may make changes to a message. The output of such an MLM is considered to be a new message; delivery of the original has been completed prior to distribution of the re-posted message. Such messages are often re-formatted, such as with list-specific header fields or other properties, to facilitate discussion among list subscribers.

authoring: An authoring MLM is one that creates the content being sent as well as initiating its transport, rather than basing it on one or more messages received earlier. This is not a "mediator" in terms of [EMAIL-ARCH] since it originates the message, but after creation, its message processing and posting behavior otherwise do match the MLM paradigm. Typically replies are not generated, or if they are, they go to a specific recipient and not back to the list's full set of recipients. Examples include newsletters and bulk marketing mail.

digesting: A special case of the resending MLM is one that sends a single message comprising an aggregation of recent MLM submissions, which might be a message of [MIME] type "multipart/digest" (see [MIME-TYPES]). This is obviously a new message but it may contain a sequence of original messages that may themselves have been DKIM-signed.

In the remainder of this document we distinguish two relevant steps, corresponding to the following SMTP transactions:

MLM Input: Originating user is author; originating ADMD is originator and signer; MLM's ADMD is verifier; MLM's input function is receiver.

MLM Output: MLM (sending its reconstructed copy of the originating user's message) is author; MLM's ADMD is originator and signer; the ADMD of each subscriber of the list is a verifier; each subscriber is a receiver.

Much of this document focuses on the resending class of MLM as it has the most direct conflict operationally with DKIM.

The dissection of the overall MLM operation into these two distinct phases allows the DKIM-specific issues with respect to MLMs to be isolated and handled in a logical way. The main issue is that the repackaging and reposting of a message by an MLM is actually the construction of a completely new message, and as such the MLM is introducing new content into the email ecosystem, consuming the author's copy of the message and creating its own. When considered in this way, the dual role of the MLM and its ADMD becomes clear.

Some issues about these activities are discussed in Section 3.6.4 of [MAIL] and in Section 3.4.1 of [EMAIL-ARCH].

3.3. Current MLM Effects On Signatures

As described above, an aliasing MLM does not affect any existing signature, and an authoring MLM is always creating new content and thus there is never an existing signature. However, the changes a resending MLM typically make affect the RFC5322.Subject header field, addition of some list-specific header fields, and/or modification of the message body. The effects of each of these on DKIM verification are discussed below.

Subject tags: A popular feature of MLMs is the "tagging" of an RFC5322.Subject field by prefixing the field's contents with the name of the list, such as "[example]" for a list called "example". Altering the RFC5322.Subject field on new submissions by adding a list-specific prefix or suffix will invalidate the signer's signature if that header field was included in the hash when creating that signature. Section 5.5 of [DKIM] lists RFC5322.Subject as one that should be covered as it contains important user-visible text, so this is expected to be an issue for any list that makes such changes.

List-specific header fields: Some lists will add header fields specific to list administrative functions such as those defined in [LIST-ID] and [LIST-URLS], or the "Resent-" fields defined in [MAIL]. It is unlikely that a typical MUA would include such fields in an original message, and DKIM is resilient to the addition of header fields in general (see notes about the "h=" tag in Section 3.5 of [DKIM]). Therefore not seen as a concern.

Other header fields: Some lists will add or replace header fields such as "Reply-To" or "Sender" in order to establish that the message is being sent in the context of the mailing list, so that the list is identified ("Sender") and any user replies go to the list ("Reply-To"). If these fields were included in the original message, it is possible that one or more of them may have been included in the signature hash, and those signatures will thus be broken.

Minor body changes: Some lists prepend or append a few lines to each message to remind subscribers of an administrative URL for subscription issues, or of list policy, etc. Changes to the body will alter the body hash computed at the DKIM verifier, so these will render any existing signatures that cover those portions of the message body unverifiable. [DKIM] includes the capability to limit the length of the body covered by its body hash so that appended text will not interfere with signature validation, but this has security implications.

Major body changes: There are some MLMs that make more substantial changes to message bodies when preparing them for re-distribution, such as adding, deleting, reordering, or reformatting [MIME] parts, "flattening" HTML messages into plain text, or inserting headers or footers within HTML messages. Most or all of these changes will invalidate a DKIM signature.

MIME part removal: Some MLMs that are MIME-aware will remove large MIME parts from submissions and replace them with URLs to reduce the size of the distributed form of the message and to prevent inadvertent automated malware delivery. Except in some cases where a body length limit is applied in generation of the DKIM signature, the signature will be broken.

There reportedly still exist some mailing lists in operation that are actually run manually by a human list manager, whose workings in preparing a message for distribution could include the above or even some other changes.

In general, absent a general movement by MLM developers and operators toward more DKIM-friendly practices, an MLM subscriber cannot expect

signatures applied before the message was processed by the MLM to be valid on delivery to a receiver. Such an evolution is not expected in the short term due to general development and deployment inertia. Moreover, even if an MLM currently passes messages unmodified such that author signatures validate, it is possible that a configuration change or software upgrade to that MLM will cause that no longer to be true.

4. Non-Participating MLMs

This section contains a discussion of issues regarding sending DKIM-signed mail to or through an MLM that is not DKIM-aware. Specifically, the header fields introduced by [DKIM] and [AUTH-RESULTS] carry no special meaning to such an MLM.

4.1. Author-Related Signing

In an idealized world, if an author knows that the MLM to which a message is being sent is a non-participating resending MLM, the author SHOULD be cautious when deciding whether or not to send a signed message to the list. The MLM could make a change that would invalidate the author's signature but not remove it prior to re-distribution. Hence, list recipients would receive a message purportedly from the author but bearing a DKIM signature that would not verify. Some mail filtering software incorrectly penalizes a message containing a DKIM signature that fails verification. This may have detrimental effects outside of the author's control. (Additional discussion of this is below.) This problem can be compounded if there are receivers that apply signing policies (e.g., [ADSP]) and the author publishes any kind of strict policy, i.e., a policy that requests that receivers reject or otherwise deal severely with non-compliant messages.

For domains that do publish strict ADSP policies, the originating site SHOULD use a separate message stream (see Section 2.5), such as a signing and author subdomain, for the "personal" mail -- a subdomain that is different from domain(s) used for other mail streams. This allows each to develop an independent reputation, and more stringent policies (including ADSP) can be applied to the mail stream(s) that do not go through mailing lists or perhaps do not get signed at all.

However, all of this presupposes a level of infrastructure understanding that is not expected to be common. Thus, it will be incumbent upon site administrators to consider how support of users wishing to participate in mailing lists might be accomplished as DKIM achieves wider adoption.

In general, the more strict practices and policies are likely to be successful only for the mail streams subject to the most end-to-end control by the originating organization. That typically excludes mail going through MLMs. Therefore, site administrators wishing to employ ADSP with a "discardable" setting SHOULD separate the controlled mail stream warranting this handling from other mail streams that are less controlled, such as personal mail that transits MLMs. (See also in Section 5.7 below.)

4.2. Verification Outcomes at Receivers

There is no reliable way to determine that a piece of mail arrived via a non-participating MLM. Sites whose users subscribe to non-participating MLMs SHOULD ensure that such user mail streams are not subject to strict DKIM-related handling policies.

4.3. Handling Choices at Receivers

In order to exempt some mail from the expectation of signature verification, as discussed in Section 4.1, receiving ADMDs would need to register non-participating lists and confirm that mail transited them. However, such an approach requires excessive effort and even then is likely to be unreliable. Hence, it is not a scalable solution.

Any treatment of a verification failure as having special meaning is a violation of the basic DKIM signing specification. The only valid, standardized basis for going beyond that specification is with specific ADSP direction.

Use of restrictive domain policies such as [ADSP] "discardable" presents an additional challenge. In that case, when a message is unsigned or the signature can no longer be verified, discarding of the message is requested. There is no exception in the policy for a message that may have been altered by an MLM, nor is there a reliable way to identify such mail. Therefore, participants SHOULD honour the policy and disallow the message.

4.4. Wrapping A Non-Participating MLM

One approach for adding DKIM support to an otherwise non-participating MLM is to "wrap" the MLM, or in essence place it between other DKIM-aware components (such as MTAs) that provide some DKIM services. For example, the ADMD operating a non-participating MLM could have its DKIM verifier act on messages from list subscribers, enforcing some of the features and recommendations of Section 5 on behalf of the MLM, and the MTA or MSA receiving the MLM Output could also add a DKIM signature for the MLM's domain.

5. Participating MLMs

This section contains a discussion of issues regarding DKIM-signed mail that transits an MLM which is DKIM-aware.

5.1. General

Changes that merely add new header fields, such as those specified by [LIST-ID], [LIST-URLS] and [MAIL], are generally the most friendly to a DKIM-participating email infrastructure. Their addition by an MLM will not affect any existing DKIM signatures unless those fields were already present and covered by a signature's hash, or a signature was created specifically to disallow their addition (see the note about "h=" in Section 3.5 of [DKIM]).

However, the practice of applying headers and footers to message bodies is common and not expected to fade regardless of what documents this or any standards body might produce. This sort of change will invalidate the signature on a message where the body hash covers the entire message. Thus, the following sections also discuss and suggest other processing alternatives.

A possible mitigation to this incompatibility is use of the "l=" tag to bound the portion of the body covered by the DKIM body hash, but this is not workable for [MIME] messages; moreover, it has security considerations (see Section 3.5 of [DKIM]). Its use is therefore discouraged.

Expressions of list-specific policy (e.g., rules for participation, small advertisements, etc.) are often added to outgoing messages by MLM operators. There is currently no header field proposed for relaying such general operational MLM details apart from what [LIST-URLS] already supports. This sort of information is commonly included footer text appended to the body of the message, or header text prepended above the original body. It is RECOMMENDED that periodic, automatic mailings to the list are sent to remind subscribers of list policy. It is also RECOMMENDED that the use of standard header fields to express list operation parameters be applied rather than body changes. These periodic mailings will be repetitive, of course, but by being generally the same each time they can be easily filtered if desired.

5.2. DKIM Author Domain Signing Practices

ADSP presents a particular challenge. An author domain posting a policy of "discardable" imposes a very tight restriction on the use of mailing lists, essentially constraining that domain's users to lists operated by aliasing MLMs only; any MLM that alters a message

from such a domain or removes its signature subjects the message to severe action by verifiers or receivers. A resending MLM SHOULD reject outright any mail from an author whose domain posts such a policy, as those messages likely to be discarded or rejected by any ADSP-aware recipients. See also the discussion in Section 5.3.

Where such rejection of "discardable" mail is not enforced, and such mail arrives to a verifier that applies ADSP checks which fail, the message SHOULD either be discarded (i.e. accept the message at the [SMTP] level but discard it without delivery) or rejected by returning a 5xx error code. In the latter case, some advice for how to conduct the rejection in a potentially meaningful way can be found in Section 5.11.

The reason for these recommendations is best illustrated by example. Suppose the following:

- users U1 and U2 are subscribers of list L;
- U1 is within an ADMD that advertises a "discardable" policy using ADSP;
- L alters submissions prior to re-sending in a way that invalidates the DKIM signature added by U1's ADMD;
- U2's ADMD enforces ADSP at the border by issuing an SMTP error code; and
- L is configured to remove subscribers whose mail is bouncing.

It follows then that a submission to L from U1 will be received at U2, but since the DKIM signature fails to verify, U2's ADMD will reject it based on the ADSP protocol. That rejection is received at L, which proceeds to remove U2 from the list.

See also Appendix B.5 of [ADSP] for further discussion.

5.3. Subscriptions

At subscription time, an ADSP-aware MLM SHOULD check for a published ADSP record for the new subscriber's domain. If the policy specifies "discardable", the MLM SHOULD disallow the subscription or present a warning that the subscriber's submissions to the mailing list might not be deliverable to some recipients because of the subscriber's ADMD's published policy.

Of course, such a policy record could be created after subscription, so this is not a universal solution. An MLM implementation MAY do

periodic checks of its subscribers and issue warnings where such a policy is detected, or simply check upon each submission.

5.4. Exceptions To ADSP Recommendations

Where an ADMD has established some out-of-band trust agreement with another ADMD such that an Authentication-Results field applied by one is trusted by the other, the above recommendations for MLM operation with respect to ADSP do not apply because it is then possible to establish whether or not a valid author signature can be inferred even if one is not present on receipt.

5.5. Author-Related Signing

An important consideration is that authors rarely have any direct influence over the management of an MLM. Specifically, the behavior of an intermediary (e.g., an MLM that is not careful about filtering out junk mail or being diligent about unsubscription requests) can trigger recipient complaints that reflect back on those agents that appear to be responsible for the message, in this case an author via the address found in the RFC5322.From field. In the future, as DKIM signature outputs (i.e., the signing domain) are used as inputs to reputation modules, there may be a desire to insulate one's reputation from influence by the unknown results of sending mail through an MLM. In that case, authors SHOULD create a mail stream specifically used for generating signatures when sending traffic to MLMs.

This suggestion can be made more general. Mail that is of a transactional or generally end-to-end nature, and not likely to be forwarded around either by MLMs or users, SHOULD be signed with a different mail stream identifier from a stream that serves more varied uses.

5.6. Verification Outcomes at MLMs

MLMs typically attempt to authenticate messages posted through them. They usually do this through the trivial (and insecure) means of verifying the RFC5322.From field email address (or, less frequently, the RFC5321.MailFrom parameter) against a list subscription registry. DKIM enables a stronger form of authentication: The MLM can require that messages using a given RFC5322.From address also have a DKIM signature with a corresponding "d=" domain. This feature would be somewhat similar to using ADSP, except that the requirement for it would be imposed by the MLM and not the author's organization.

(Note, however, that this goes beyond DKIM's documented semantics. It is presented as a possible workable enhancement.)

As described, the MLM might conduct DKIM verification of a signed message to attempt to confirm the identity of the author. Although it is a common and intuitive conclusion, few signed messages will include an author signature (see [ADSP]). MLM implementers adding such support would have accommodate this. For example, an MLM might be designed to accommodate a list of possible signing domains (the "d=" portion of a DKIM signature) for a given author, and determine at verification time if any of those are present. This enables a more reliable method of authentication at the expense of having to store a mapping of authorized signing domains for subscribers and trusting that it will be kept current.

A message that cannot be thus authenticated MAY be held for moderation or rejected outright.

This logic could apply to any list operation, not just list submission. In particular, this improved authentication MAY apply to subscription, unsubscription, and/or changes to subscriber options that are sent via email rather than through an authenticated, interactive channel such as the web.

In the case of verification of signatures on submissions, MLMs SHOULD add an [AUTH-RESULTS] header field to indicate the signature(s) observed on the submission as it arrived at the MLM and what the outcome of the evaluation was. Downstream agents might or might not trust the content of that header field depending on their own a priori knowledge of the operation of the ADMD generating (and, preferably, signing) that header field. See [AUTH-RESULTS] for further discussion.

5.7. Signature Removal Issues

A message that arrives signed with DKIM means some domain prior to MLM Input has made a claim of some responsibility for the message. An obvious benefit to leaving the input-side signatures intact, then, is to preserve that original assertion of responsibility for the message so that the receivers of the final message have an opportunity to evaluate the message with that information available to them.

However, if the MLM is configured to make changes to the message prior to re-posting that would invalidate the original signature(s), further action is RECOMMENDED to prevent invalidated signatures from arriving at final recipients, possibly triggering unwarranted filter actions. (Note, however, that such filtering actions are plainly wrong; [DKIM] stipulates that an invalid signature is to be treated as no signature at all.)

A possible solution would be to:

1. Attempt verification of all DKIM signatures present on the input message;

2. Apply local policy to authenticate the identity of the author;

3. Remove all existing [AUTH-RESULTS] fields (optional);

4. Add an [AUTH-RESULTS] header field to the message to indicate the results of the above;

5. Remove all previously-evaluated DKIM signatures;

6. Affix a new signature that includes in in its hashes the entire message on the output side, including the Authentication-Results header field just added (see Section 5.8).

Removing the original signature(s) seems particularly appropriate when the MLM knows it is likely to invalidate any or all of them due to the nature of the reformatting it will do. This avoids false negatives at the list's subscribers in their roles as receivers of the message; although [DKIM] stipulates that an invalid signature is the same as no signature, it is anticipated that there will be some implementations that ignore this advice.

The MLM could re-evaluate existing signatures after making its message changes to determine whether or not any of them have been invalidated. The cost of this is reduced by the fact that, presumably, the necessary public keys have already been downloaded and one or both of the message hashes could be reused.

Per the discussion in [AUTH-RESULTS], a receiver's choice to put any faith in the veracity of that header field requires an a priori assessment of the agent that created it. Absent that assessment, a receiver cannot interpret the field as valid. Thus, the final recipients of the message have no way to verify on their own the authenticity of the author's identity on that message. However, if that field is the only one on the message when the verifier gets it, and the verifier explicitly trusts the signer that included the Authentication-Results field in its header hash (in this case, the MLM), the verifier is in a position to believe that a valid author signature was present on the message.

This can be generalized as follows: A receiver SHOULD consider only [AUTH-RESULTS] fields bearing an authserv-id that appears in a list of sites the receiver trusts and which is also included in the header hash of a [DKIM] signature added by a domain in the same trusted

list.

Since an aliasing MLM makes no substantive changes to a message, it need not consider the issue of signature removal as the original signatures should arrive at least to the next MTA unmodified. It is possible that future domain-based reputations would prefer a more rich data set on receipt of a message, and in that case signature removal would be undesirable.

An authoring MLM is closed to outside submitters, thus much of this discussion does not apply in that case.

5.8. MLM Signatures

DKIM-aware resending MLMs and authoring MLMs SHOULD affix their own signatures when distributing messages. The MLM is responsible for the alterations it makes to the original messages it is re-sending, and should express this via a signature. This is also helpful for getting feedback from any FBLs that might be set up so that undesired list mail can generate appropriate action.

MLM signatures will likely be used by recipient systems to recognize list mail, and they give the MLM's ADMD an opportunity to develop a good reputation for the list itself.

A signing MLM is, as any other MLM, free to omit redistribution of a message if that message was not signed in accordance with its own local configuration or policy. It could also redistribute but not sign such mail. However, selective signing is NOT RECOMMENDED; essentially that would create two message streams from the MLM, one signed and one not, which can confuse DKIM-aware verifiers and receivers.

A signing MLM could add a List-Post: header field (see [LIST-URLS]) using that DNS domain matching the one used in the "d=" tag of the DKIM signature that is added by the MLM. This can be used by verifiers or receivers to identify the DKIM signature that was added by the MLM. This is not required, however; it is believed the reputation of the signer will be a more critical data point rather than this suggested binding. Furthermore, this is not a binding recognized by any current specification document.

A DKIM-aware resending MLM SHOULD sign the entire message after the message is prepared for distribution (i.e. the "MLM Output" from Section 3.2). Any other configuration might generate signatures that will not validate.

DKIM-aware authoring MLMs MUST sign the mail they send according to

the regular signing guidelines given in [DKIM].

One concern is that having an MLM apply its signature to unsigned mail might cause some verifiers or receivers to interpret the signature as conferring more authority or authenticity to the message content than is defined by [DKIM]. This is an issue beyond MLMs and primarily entails receive-side processing outside of the scope of [DKIM]. It is nevertheless worth noting here.

5.9. Verification Outcomes at Final Receiving Sites

In general, verifiers and receivers SHOULD treat a signed message from an MLM like any other signed message; indeed, it would be difficult to discern any difference since specifications such as [LIST-URLS] and [LIST-ID] are not universally deployed and can be trivially spoofed.

However, because the author domain will commonly be different from the MLM's signing domain, there may be a conflict with [ADSP] as discussed in Section 4.3 and Section 5.7, especially where an ADMD has misused ADSP.

5.10. Use With FBLs

An FBL operator might wish to act on a complaint from a user about a message sent to a list. Some FBLs could choose to generate feedback reports based on DKIM verifications in the subject message. Such operators SHOULD send a report to each domain with a valid signature that has an FBL agreement established, as DKIM signatures are claims of some responsibility for that message. Because authors generally have limited control over the operation of a list, this point makes MLM signing all the more important.

MLM operators SHOULD register with FBLs from major service providers. In the context of DKIM, there SHOULD be an exchange of information with the FBL provider including what signing domain the MLM will use, if any.

Where the FBL wishes to be more specific, it MAY act solely on a DKIM signature where the signing domain matches the DNS domain found in a List-Post: header field (or similar).

Use of FBLs in this way SHOULD be made explicit to list subscribers. For example, if it is the policy of the MLM's ADMD to handle an FBL item by unsubscribing the user that was the apparent sender of the offending message, advising subscribers of this in advance would help to avoid surprises later.

A DKIM-signed message sent to an MLM, and then distributed to all of a list's recipients, could result in a complaint from one of the final recipients for some reason. This could be an actual complaint from some subscriber that finds the message abusive or otherwise undesirable, or it could be an automated complaint such as receiver detection of an invalidated DKIM signature or some other condition. It could also be a complaint that results from antagonistic behaviour, such as is common when a subscriber to a list is having trouble unsubscribing, and then begins issuing complaints about all submissions to the list. This would result in a complaint being generated in the context of an FBL report back to the message author. However, the original author has no involvement in operation of the MLM itself, meaning the FBL report is not actionable, and is thus undesirable.

5.11. Handling Choices at Receivers

A recipient that explicitly trusts signatures from a particular MLM MAY wish to extend that trust to an [AUTH-RESULTS] header field signed by that MLM. The recipient MAY then do additional processing of the message, using the results recorded in the Authentication-Results header field instead of the original author's DKIM signature. This includes possibly processing the message as per ADSP requirements.

Receivers SHOULD ignore or remove all unsigned externally-applied Authentication-Results header fields, and those not signed by an ADMD that can be trusted by the receiver. See Section 5 and Section 7 of [AUTH-RESULTS] for further discussion.

Upon DKIM and ADSP evaluation during an SMTP session (a common implementation), an agent MAY decide to reject a message during an SMTP session. If this is done, use of an [SMTP] failure code not normally used for "user unknown" (550) is preferred; therefore, 554 SHOULD be used. If the rejecting SMTP server supports [ENHANCED] status codes, it SHOULD make a distinction between messages rejected deliberately due to policy decisions rather than those rejected because of other delivery issues. In particular, a policy rejection SHOULD be relayed using a 5.7.1 enhanced status code and some appropriate wording in the text part of the reply, in contrast to a code of 5.1.1 indicating the user does not exist. Those MLMs that automatically attempt to remove users with prolonged delivery problems (such as account deletion) SHOULD thus detect the difference between policy rejection and other delivery failures, and act accordingly. SMTP servers doing so SHOULD also use appropriate wording in the text portion of the reply, perhaps explicitly using the string "ADSP" to facilitate searching of relevant data in logs.

The preceding paragraph does not apply to an [ADSP] policy of "discardable". In such cases where the submission fails that test, the receiver or verifier SHOULD discard the message but return an SMTP success code, i.e. accept the message but drop it without delivery. An SMTP rejection of such mail instead of the requested discard action causes more harm than good.

6. DKIM Reporting

As mechanisms become available for reporting forensic details about DKIM verification failures, MLMs will benefit from their use.

MLMs SHOULD apply DKIM failure reporting mechanisms as a method for providing feedback to signers about issues with DKIM infrastructure. This is especially important for MLMs that implement DKIM verification as a mechanism for authentication of list configuration commands and submissions from subscribers.

7. IANA Considerations

This document includes no IANA actions. It should be removed prior to publication.

8. Security Considerations

This document provides suggested or best current practices for use with DKIM, and as such does not introduce any new technologies for consideration. However, the following security issues should be considered when implementing the above practices.

8.1. Security Considerations from DKIM and ADSP

Readers should be familiar with the material in the Security Considerations in [DKIM], [ADSP] and [AUTH-RESULTS] as appropriate.

8.2. Authentication Results When Relaying

Section 5 advocates addition of an [AUTH-RESULTS] header field to indicate authentication status of a message received as MLM Input. Per Section 7.2 of [AUTH-RESULTS], receivers generally should not trust such data without a good reason to do so, such as an a priori agreement with the MLM's ADMD.

Such agreements are strongly advised to include a requirement that those header fields be covered by a [DKIM] signature added by the MLM's ADMD.

9. References

9.1. Normative References

[ADSP] Allman, E., Delany, M., Fenton, J., and J. Levine, "DKIM Sender Signing Practises", RFC 5617, August 2009.

[AUTH-RESULTS] Kucherawy, M., "Message Header Field for Indicating Message Authentication Status", RFC 5451, April 2009.

[DKIM] Crocker, D., Hansen, T., and M. Kucherawy, "DomainKeys Identified Mail (DKIM) Signatures", I-D draft-ietf-dkim-rfc4871bis, April 2011.

[EMAIL-ARCH] Crocker, D., "Internet Mail Architecture", RFC 5598, July 2009.

[KEYWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[MAIL] Resnick, P., "Internet Message Format", RFC 5322, October 2008.

9.2. Informative References

[ARF] Shafranovich, Y., Levine, J., and M. Kucherawy, "An Extensible Format for Email Feedback Reports", RFC 5965, August 2010.

[DKIM-DEPLOYMENT] Hansen, T., Siegel, E., Hallam-Baker, P., and D. Crocker, "DomainKeys Identified Mail (DKIM) Development, Deployment and Operations", I-D DRAFT-IETF-DKIM-DEPLOYMENT, January 2010.

[DKIM-OVERVIEW] Hansen, T., Crocker, D., and P. Hallam-Baker, "DomainKeys Identified Mail (DKIM) Service Overview", RFC 5585, July 2009.

[ENHANCED] Vaudreuil, G., "Enhanced Mail System Status Codes", RFC 3463, January 2003.

[IODEF] Danyliw, R., Meijer, J., and Y. Demchenko, "The Incident

Object Description Exchange Format", RFC 5070, December 2007.

[LIST-ID] Chandhok, R. and G. Wenger, "List-Id: A Structured Field and Namespace for the Identification of Mailing Lists", RFC 2919, March 2001.

[LIST-URLS] Neufeld, G. and J. Baer, "The Use of URLs as Meta-Syntax for Core Mail List Commands and their Transport through Message Header Fields", RFC 2369, July 1998.

[MIME] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996.

[MIME-TYPES] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", RFC 2046, November 1996.

[SMTP] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, October 2008.

Appendix A. Acknowledgements

The author wishes to acknowledge the following for their review and constructive criticism of this document: Serge Aumont, Daniel Black, Dave Crocker, J.D. Falk, Tony Hansen, Eliot Lear, Charles Lindsey, John Levine, Jeff Macdonald, S. Moonesamy, Rolf E. Sonneveld, and Alessandro Vesely.

Appendix B. Example Scenarios

This section describes a few MLM-related DKIM scenarios that were part of the impetus for this work, and the recommended resolutions for each.

B.1. MLMs and ADSP

Problem:

- author ADMD advertises an ADSP policy of "dkim=discardable"
- author sends DKIM-signed mail to a non-participating MLM, which invalidates the signature
- receiver MTA checks DKIM and ADSP at SMTP time, and is configured to reject ADSP failures, so rejects this message
- process repeats a few times, after which the MLM unsubscribes the receiver

Solution: MLMs should refuse mail from domains advertising ADSP policies of "discardable" unless the MLMs are certain they make no changes that invalidate DKIM signatures.

B.2. MLMs and FBLs

Problem:

- subscriber sends signed mail to a non-participating MLM that does not invalidate the signature
- a recipient reports the message as spam
- FBL at recipient ADMD sends report to contributor rather than list manager

Solution: MLMs should sign mail they send and might also strip existing signatures; FBLs should report to list operators instead of subscribers where such can be distinguished, otherwise to all parties with valid signatures.

Author's Address

Murray S. Kucherawy
Cloudmark
128 King St., 2nd Floor
San Francisco, CA 94107
US

Phone: +1 415 946 3800
Email: msk@cloudmark.com