Network Working Group
Internet-Draft
Intended status: Experimental
Expires: October 12, 2015

M. Kucherawy

D. Crocker
Brandenburg InternetWorking

April 10, 2015

Delegating DKIM Signing Authority
draft-kucherawy-dkim-delegate-02

Abstract

DomainKeys Identified Mail (DKIM) permits a handling agent to affix a digital signature to an email message, associating a domain name with that message using cryptographic signing techniques. The digital signature typically covers most of a message's original portions, although the specific choices for content hashing are at the discretion of the signer. DKIM signatures survive simply email relaying but typically are invalidated by processing through Mediators, such as mailing lists. For such cases, the signer needs a way to indicate that a valid signature from some third party was anticipated, and constitutes an acceptable handling of the message. This enables a receiver to conclude that the content is legitimately from that original signer, even though its original signature no longer validates.

This document defines a mechanism for improving the ability to assess DKIM validity for such messages.

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 October 12, 2015.

Copyright Notice

Table of Contents

1. Background

DomainKeys Identified Mail [RFC6376] defines a mechanism whereby a verified domain name can be attached to a message, using a cryptographic signature. It does not, however, assert that this domain name matches a domain name found anywhere else in the message.

DKIM signature survival is usually successful through basic email relaying nodes. It also survives simple Mediators, such as mailbox forwarding agents, because they only modify the message envelope and do not modify the original message header or body. Transit through other Mediators, such as mailing lists, is usually problematic, because they modify portions of the message covered by the signature and therefore invalidate it.

When a receiver needs to determine whether a message was legitimately processed by a purported original signer, a mechanism is needed that is more likely to survive transit through Mediators. This need is especially strong for environments wishing to enforce policy linkage between the author, the author's domain and specific email service providers, such as when the latter two are the same. An example of such a need is when that original signer publishes policies concerning the use of its domain name. Examples are ADSP [RFC5617] and DMARC [I-D.KUCHERAWY-DMARC-BASE]. These policies cannot be applied properly when legitimate mail for the original signer's domain cannot be validated by the final Receiver. The potential for malfunction otherwise is described in Section 5.2 of [RFC6377].

The issues with mailing lists and similar re-mailing applications can be resolved by a mechanism that permits the original signer's domain ("A") to indicate that some other domain ("B") is explicitly permitted to re-sign content generated by "A", such that a Receiver can observe signaling from both "A" and "B" that this relationship exists.

An experimental attempt to do this appeared in [RFC6541]. The method presented there imposes a burden on the original signing domain to publish those relationships a priori, via the DNS. This proved cumbersome with poor scaling properties. So, a mechanism that does not have such an external dependency is preferred.

2. Definitions

Numerous terms used here, especially "Author", "Originator", "Receiver", and "Recipient", are defined in [RFC5598]. DKIM-related terminology, such as "Signing Domain", are taken from the DKIM specification [RFC6376].

3. DKIM-Delegate Specification

An email header field, called "DKIM-Delegate", is defined. When present, it asserts an ephemeral relationship between an original message signing domain and a later intermediary (Mediator).

3.1. Design Summary

An "Original Signer" (typically the Originator serving the Author) affixes a DKIM signatures to a message using whatever parameters it wishes. In addition to this, it affixes a DKIM-Delegate field that indicates an ephemeral relationship exists between the Author domain and some set of other domains that are expected to handle the message. Preferably, the Mediator also signs the message, to provide a reliable confirmation of handling by that Mediator. If a Receiver finds that the Original Signer's "normal" signature does not validate or is missing, it can perform DKIM-Delegate evaluation.

The DKIM-Delegate field includes a hash and a cryptographic signature, just like DKIM-Signature fields do. However, the only content covered by the hash is the DKIM-Delegate field and its parameters.

In combination with DKIM signatures, this mechanism can aid a receiver in assessing whether the message was legitimately handled by the intermediary and whether the message was likely to have had a legitimate signature by the original signing domain, even when that original signature became invalid. This makes it possible to identify such messages separately from those without these assurances, and thus permits treating the latter with more skepticism.

3.2. Mechanism

The specific mechanism operates as follows:

1. A "Primary" DKIM Signature is affixed to a message by a handling agent, identifying the Originator's domain and using typical signing choices, such as covering the entire message content in the body hash. (That is, it does not use the "l=" tag.)

2. The signer adds a DKIM-Delegate header field identifying the Originator's domain. It also identifies the specific domain(s) with which it wishes to claim an ephemeral relationship. The DKIM-Delegate field is self-signed, as described below.

3. The Originator transmits the message to the Receiver in the usual way.

4. If the Receiver is not a Mediator, then normal DKIM processing occurs, and DKIM-Delegate is ignored.

5. An authorized Mediator SHOULD affix its own, normal DKIM signature to the message after making any content modifications it is configured to make and before re-sending the message to new Receiver(s).

6. The new Receiver attempts to validate the Primary signature affixed by the original signer. If it is valid, the requirements of this protocol are satisfied (and the algorithm terminates here).

7. The new Receiver attempts to validate the DKIM-Delegate field affixed by the original signer. If it is not valid, expired, or absent, the requirements of this protocol cannot be satisfied (and the algorithm terminates here).

8. The Receiver extracts the list of domains authorized to re-sign for the Author domain from the "t=" tag of the DKIM-Delegate field. Call this set "D".

9. The Receiver performs normal validation checks of all other DKIM signatures on the message that include the entire message body in their body hashes, and stores the set of domains from passing signatures in set "S".

10. If the intersection of "D" and "S" is not empty, the requirements of this protocol are satisfied; otherwise, the requirements are not satisfied.

3.3. Syntax

The content of the DKIM-Delegate header field is a tag-list as defined in Section 3.2 of [RFC6376]. The valid tags are:

a= Signature algorithm (plain-text; REQUIRED). As in Section 3.5 of [RFC6376], this contains a string that describes the signature generation algorithm used by the signer.

b= Signature data (base64; REQUIRED). As in Section 3.5 of [RFC6376], this contains a digital signature of the content of this header field. The same syntax rules for DKIM signatures apply here.

d= Author domain (plain-text; REQUIRED). This value names the domain of the Author, which is delegating signing authority to one or more other domains.

s= Selector name (plain-text; REQUIRED). As in Section 3.5 of [RFC6376], this names a particular public/private key pair that is used to sign and verify the content of this header field. It will be used to construct a DNS query for a text representation of the public key.

t= Delegation target (plain-text; REQUIRED). This value is a comma-separated list of domain names to which the authority to sign on behalf of the Author domain is being delegated.

x= Expiration time (plain-text unsigned decimal integer; RECOMMENDED, default is no expiration) As in Section 3.5 of [RFC6376], this specifies a timestamp beyond which this header field MAY be considered invalid.

As with DKIM itself, any other tag MUST be ignored.

3.4. Preparation

The content of a DKIM-Delegate field is prepared for signing by applying the "relaxed" header canonicalization scheme defined in Section 3.4.2 of [RFC6376] and the algorithm described in Section 3.7. For DKIM-Delegate, the only content that is hashed is the constructed DKIM-Delegate field itself, with an empty "b=" tag; notably, there is no "v=" or "bh=" tag, so these are omitted. The signature, once generated, is then added as the value of the "b=" tag.

The Original Signer SHOULD use the same selector (and, hence, signing key) for DKIM-Delegate fields as it uses for Primary signatures so that Domain Name Service caching can be used.

3.5. Verification

A Receiver verifies the DKIM-Delegate field by applying the general algorithm described in Section 6.1 of [RFC6376] with the following caveats:

- This specification has a subset of the tags found in a DKIM-Signature. Most notably, DKIM-Delegate has no "v=", "bh=", "c=", or "h=" tag.

A DKIM-Delegate field that verifies contains an explicit list of domains authorized to sign content for the Author domain. The

Receiver then simply ensures that there is a valid DKIM-Signature from one of the delegated domains before concluding that the Author domain approved the content.

4. Expiration

The expiration time on the DKIM-Delegate field needs to be long enough to permit evaluation by Receivers of the re-submitted message, yet short enough to limit the potential for unauthorized injection attacks. A good choice is a small number of days or even hours.

If abuse is detected, the owner of the Author domain can remove the key from publication in the DNS as a way of revoking that key and thus invalidating any unverified DKIM-Delegate fields.

5. Discussion

The use of the Primary signature ensures that if the original message arrives unmodified, the Receiver is assured of its legitimacy as having been generated and sent by the original signer, irrespective of what Mediator handled it.

Mediators, such as mailing list software, commonly make adjustments to a message prior to re-submitting it for transfer to final recipients. Adjustments often include prepending list-identifying material to the Subject field, or appending URIs and such to the message body referring Receivers to further information about the list itself. This will almost always invalidate the Primary signature, so downstream receivers cannot be sure (via DKIM, at least) where the message originated.

6. Security Considerations

Use of this header field (and DKIM as described here) amounts to an ephemeral granting of the ability for the first Receivers (typically the Mediators named in the To and Cc fields) to generate content that the ultimate Receivers will consider valid on behalf of the Author. A compromised Mediator can thus replace the original content in its entirety while still satisfying this protocol.

The "t=" tag might be used to name Mediators that do not appear in the To or Cc fields of a message, which means they would normally appear in the message envelope only. Thus, use of that tag records envelope details in the message, which could be information intended to be kept private.

As described in Section 3.2, this mechanism signature presents a time-limited but nevertheless present opportunity for someone at the

Mediator's domain to generate content apparently authorized by the Author domain.

Given the exposures described above, message originators would do well to consider limiting use of this protocol to those messages that will transit trusted Mediators only. Determining which Mediators are worthy of such trust is a local policy matter, outside of the scope of this document.

7. IANA Considerations

IANA is requested to make the following new entry in the Permanent Message Header Field Names registry, per [RFC3864]:

Header field name: DKIM-Delegate
Applicable protocol: mail ([RFC5322])
Status: Experimental
Author/Change controller: IETF
Specification document(s): [this document]
Related information:
Requesting review of any proposed changes and additions to this field is recommended.

8. References

8.1. Normative References

[RFC3864] Klyne, G., Nottingham, M., and J. Mogul, "Registration Procedures for Message Header Fields", BCP 90, RFC 3864, September 2004.

[RFC6376] Crocker, D., Hansen, T., and M. Kucherawy, "DomainKeys Identified Mail (DKIM) Signatures", STD 76, RFC 6376, September 2011.

8.2. Informative References

[I-D.KUCHERAWY-DMARC-BASE] Kucherawy, M., Ed. and E. Zwicky, Ed., "Domain-based Message Authentication, Reporting and Conformance (DMARC)", I-D draft-kucherawy-dmarc-base.

[RFC5598] Crocker, D., "Internet Mail Architecture", RFC 5598, July 2009.

[RFC5617] Allman, E., Fenton, J., Delany, M., and

J. Levine, "DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP)", RFC 5617, August 2009.

[RFC6377] Kucherawy, M., "DomainKeys Identified Mail (DKIM) and Mailing Lists", BCP 167, RFC 6377, September 2011.

[RFC6541] Kucherawy, M., "DomainKeys Identified Mail (DKIM) Authorized Third-Party Signatures", RFC 6541, February 2012.

Appendix A. Example

Given the following message header (numbers in braces are line numbers):

```
{1}  From: somebody@example.com
{2}  To: mailinglist@ietf.example
{3}  Subject: What's up with DKIM?
{4}  Date: Thu, 12 Jun 2014 11:08:10 -0700
{5}  DKIM-Signature: v=1; s=rashani; d=example.com;
{6}      h=from:to:subject:date; ...
{7}  DKIM-Delegate: a=rsa-sha256; d=example.com; s=rashani;
{8}      x=1402686254; t=ietf.example; b=<base64-data>
{9}
{10} [message body omitted]
```

The DKIM signature (line 5) is an Author signature that covers the entire message body (the "Primary" signature). If it validates on delivery, the remainder of the DKIM material can be ignored.

There is also a DKIM-Delegate header field (line 7) that identifies the delegating party in its "d=" tag. It states that signing authority is delegated by "example.com" to "ietf.example" (the Mediator domain). The integrity of this field is assured by the fact that its signature verified.

On receipt at the Mediator, both signatures will typically validate. The Mediator then augments the content as needed and re-sends the message for delivery, this time adding its own signature:

```
{1}  From: somebody@example.com
{2}  To: mailinglist@ietf.example
{3}  Subject: What's up with DKIM?
{4}  Date: Thu, 12 Jun 2014 11:08:10 -0700
{5}  DKIM-Signature: v=1; s=rashani; d=example.com;
{6}      h=from:to:subject:date; ...
{7}  DKIM-Delegate: a=rsa-sha256; d=example.com; s=rashani;
{8}      x=1402686254; t=ietf.example; b=<base64-data>
{9}  List-Id: mailinglist.ietf.example
{10} DKIM-Signature: v=1; s=evetastic; d=ietf.example;
{11}     h=from:to:subject:date:dkim-delegate:list-id; ...
{12}
{13} [augmented message body omitted]
```

Because of the changed content, the Primary signature no longer validates. However, the Mediator signature will presumably validate on receipt, since it covers all of the modified content. In addition, the DKIM-Delegate field would be expected to validate as it is unlikely to be altered by Mediators.

The Receiver of this message (a list subscriber, in this case) can conclude that the following are true, based on the remaining valid signatures:

1. "example.com" authorized "ietf.example" to sign mail on its behalf;

2. "ietf.example" signed the altered content, thus taking some responsibility for it;

3. This chain of handling satisfies the need for the Author domain to have signed the message; the original message may have been modified or replaced, but such action was explicitly approved by the Author domain.

Appendix B. To-Do List

Stuff to be done:

- (nothing right now)

Some suggestions from others:

- Perhaps this is better done by one or more new DKIM-Signature tags and/or a version change. (From John Levine)

Appendix C. Acknowledgments

The authors wish to acknowledge Steve Atkins, Barry Leiba, Pete Resnick, Hector Santos, Stephen Turnbull, Alessandro Vesely, (other names) for their comments during the development of this document.

Authors' Addresses

Murray S. Kucherawy

EMail: superuser@gmail.com

D. Crocker
Brandenburg InternetWorking
675 Spruce Dr.
Sunnyvale 94086
USA

Phone: +1.408.246.8253
EMail: dcrocker@bbiw.net
URI: http://bbiw.net