Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: 27 November 2025

D. Crocker
Brandenburg Internetworking

26 May 2025

DomainKeys Originator Recipient (DKOR)
draft-crocker-dkim-dkor-00

Abstract

DKIM associates a domain name with a message stream, using cryptographic methods, to permit reliable and accurate reputation-oriented analysis of the stream. It is possible for an authorized user to conspire for additional distribution of a message, leveraging the domain name reputation for promoting spam. This is called DKIM Replay. DKOR defines a means of limiting that ability, by associating original addressing information with the message's DKIM signature, to detect distribution beyond the intended recipient. DKOR uses existing DKIM services and only requires implementation of the additional DKOR features by the signer and any receiving site wishing to participate in DKOR services. Other DKIM receivers can successfully process the same DKIM signature without knowledge of DKOR.

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 27 November 2025.

Table of Contents

1. Introduction 2
2. Framework and Terminology 3
3. Requirements 4
4. DKOR Overview 4
5. DKOR Design 5
6. DKOR Header Field 6
7. Signing Behavior 6
8. Evaluating Behavior 7
9. IANA Considerations 7
10. Security Considerations 8
11. References 8
11.1. Normative References 8
11.2. Informative References 8
Appendix A. Examples 9
A.1. Basic DKOR 9
A.2. Through an Alias 9
A.3. Through a Mailing List 9
A.4. Multiple Mailing Lists 9
A.5. Third-Party Originator 9
Acknowledgements 10
Author's Address 10

1. Introduction

DKIM [RFC6376] associates a domain name with a message stream, using cryptographic methods, to permit reliable and accurate reputation-oriented analysis of the stream. Each message in the stream has a DKIM digital signature attached to it, using the domain name. Receiving sites can then develop a reputation analysis for messages in that stream, without concern that a message was created by an unauthorized actor.

However, it is possible for an authorized user of a platform, which is signing messages with a domain name, to conspire for additional distribution of a message, beyond the set of recipients that were included at the time of original posting. The message goes through an additional platform, which then redistributes the message, while

preserving the original DKIM signature. Reception and delivery of the message to these additional recipients is aided by the reputation of the domain name used in the DKIM signature. This capability can, therefore, be used for spamming, and is called "DKIM Replay".

Ideally, authorized users of a platform are subject to sufficient controls and accountability, so their likelihood -- or even ability -- to effect this abuse is severely limited. Unfortunately, operational realities on some platforms do not achieve such control. There is therefore a need for an additional mechanism, to aid detection of DKIM Replay and to facilitate differential handling of such messages, during email transit.

Extensive community discussion converged on the view that a useful line of effort, for enabling this detection, is to include the email envelope address (e.g., SMTP RCPT-TO) [RFC5321] as part of the DKIM hash calculation. There is also interest in similarly encoding the email envelope notification return address (e.g., SMTP MAIL FROM), with the view that this might be helpful in efforts to limit use of the return 'channel' as a spamming path, called backscatter.

| [Comment:
| Including the return address (still) needs a more complete explanation. I gather it is for backscatter control, but am not at all clear on how it will get used to achieve that. So its inclusion here is as a placeholder, pending further discussion and clarifying text. /d]

2. Framework and Terminology

Internet Mail has an extensive architecture and rich associated vocabulary. Unless otherwise indicated, email terminology and reference to functional components are taken from: [RFC5598]

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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

Reference to SMTP in this document is strictly informative. Nothing in this specification is dependent upon the specific email transport service details, other than being able to obtain recipient and return address information.[RFC5598]

The means for obtaining recipient address and return address are outside the scope of this specification.

3. Requirements

Assessing the nature and legitimacy of a received message entails a complex and imperfect process. It typically includes a variety of information, derived from a variety of sources, using a variety of methods. This specification seeks to satisfy a narrow and specific part of these broad requirements. Other methods will be separate and complementary to this.

This specification assists a receiving system in detecting:

* Whether a message has been sent to an address that differs from one originally specified at the time of first posting

* What the original recipient and return addresses were

* What new recipient and return addresses are (or were, in the case of changes at multiple points along the transit path)

* What site(s) made the change(s)

4. DKOR Overview

Domain Keys Originator Recipient (DKOR) uses the existing DKIM mechanism, which develops a basic digital signature, over a specified set of message data. DKOR permits basic detection of message re-submission, upon implementation of DKOR by the signers and any receiving sites wishing to participate in DKOR services. DKOR's essential mechanism is inclusion of recipient and return addresses into the message object, by the originating site and by each re-submission point along the transit path.

A given message might be subject to multiple, legitimate re-submissions, such as through alias and mail list sites. As each of these adopts DKOR, the message will be able to provide additional information about the addressing changes it has been subject to. This enables receivers to make more accurate and reliable assessments about message handling. However, use of DKOR needs to accomodate incremental, uncoordinated, and piecemeal adoption. So for example, a message that does go through multiple, legitimate resubmissions might produce DKOR-based information from only some of the sites in the sequence.

Because DKOR relies on the existing DKIM mechanisms, other DKIM receivers that have not adopted DKOR can, nonetheless, process the same DKIM signature without knowledge of DKOR.

Hence, DKOR is an incremental and compatible enhancement to the existing DKIM email infrastructure.

5. DKOR Design

A message covered by DKOR is restricted to having a single recipient address.

DKOR defines a use of DKIM, with the DKIM signature covering whatever other header fields it is normally used to cover. For DKOR, it also covers one header field that specifies the original recipient address and the envelope notifications return address. These addresses are redundant with the addresses in their corresponding envelope fields/commands.

The presence of the DKOR header field self-declares the use of DKOR. Further there is no benefit in having the signer publish that it uses DKOR. Note that having a transit site simply remove a DKOR header field does not accomplish an effective downgrade attack, since it will cause the associated DKIM signature to fail.

The method for obtaining envelope information, to be used by DKOR, is a matter of local implementation and is outside the scope of this specification.

If the addresses in the DKOR field match those in their corresponding envelope fields/commands, and the DKIM signature validates, then DKOR passes. If either does not match, or the DKIM evaluation fails, then DKOR fails.

Policies and actions that apply to the handling of messages that pass or fail DKOR are local matters for the evaluating service and are outside the scope of this specification.

An example of challenges in determining the handling of a DKOR failure is that the failure can be the result of entirely legitimate reasons, such as a legitimate redistribution service that does not make changes to message content and only uses a new recipient address. Failures can also occur due to the considerable vagaries of email handling idiosyncrasies.

Note:
The header field used by this specification is independent of any other header fields that might contain the same addresses, in order to avoid any potential confusion about semantics or purpose.

6. DKOR Header Field

| [Comment:
| The design of the field is now derived from draft-gondwana-dkim2-header-00, merging the information into a single header field, and adding sequence numbering, to show the transit path.
| The exchange with Bron swayed me to have this support a sequence of DKOR header fields, and have them label their sequence. /d]

The DKOR header field specifies a single recipient address and a single return address. It also indicates the order in which the field was created, in the DKOR handling sequence of the message. Since DKOR support cannot be assumed for every MTA and intermediary in the transit path, the DKOR order might not reflect all of the nodes the message transited.

Field identifier	Explanation
i=	Sequence Number (from 1 to N), with 1 assigned by the originating site, and incremented for each additional DKOR header field that is added, after that (Required)
t=	Timestamp, indicating when the DKOR field was added (Optional)
mf=	The envelope return address (typically RFC5321.mail-from) present when the header field was created (Required, see below)
rt=	The envelope destination address (typically RFC5321.rcpt-to) present when the header field was created (Required, see below)

Table 1

At least one of mf or rt attributes MUST be specified.

7. Signing Behavior

1. If the recipient address (e.g., RFC5321.rcpt-to) is to be protected, obtain that envelope address and place a copy of it into the rt attribute of the DKOR header field. [RFC5322]

2. If the return address (e.g., RFC5321.mail-from) is to be protected, obtain that envelope) address and place a copy of it into the mf attribute of the DKOR header field.

3. DKOR permits either or both attributes to be present, and requires at least one.

4. Create a DKIM signature that includes the DKOR header field.

8. Evaluating Behavior

1. If a DKOR header field is present, then perform a DKOR evaluation.

2. Obtain the envelope address values used by DKOR.

3. Compare the values to the corresponding DKOR header field attribute values.

4. If either value does not match, then DKOR fails.

5. Perform a DKIM validation that includes the DKOR header field.

6. If DKIM validation fails, then DKOR fails.

9. IANA Considerations

IANA is requested to register the "DKOR" header field in the Permanent Message Header field Registry.

Header field name	DKOR
Applicable protocol	mail
Status	standard
Author/Change controller	IETF
Specification document(s)	This specification
Related information	none

Table 2

10. Security Considerations

This specification defines a mechanism for detecting retransmission of a message, that sends it to additional addressees, while preserving a DKIM signature from its original posting. The incremental security considerations are accuracy of creating and evaluating the two address fields defined here.

As with other email assessment mechanisms and the heuristics they use, DKOR creates opportunities for false positives, which can produce hostile treatment of legitimate email.

There are no other security considerations that result from using DKOR.

11. References

11.1. Normative References

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

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

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC3864] Klyne, G., Nottingham, M., and J. Mogul, "Registration Procedures for Message Header Fields", BCP 90, RFC 3864, DOI 10.17487/RFC3864, September 2004, <https://www.rfc-editor.org/info/rfc3864>.

11.2. Informative References

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

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

Appendix A. Examples

Thes show assorted DKOR header field usage examples.

A.1. Basic DKOR

Simple path from originator to recipient.

DKOR: i=1; mf=brong@fastmailteam.com; rt=dhc@dcrocker.net

A.2. Through an Alias

Routed through an aliasing site.

DKOR: i=1; mf=brong@fastmailteam.com; rt=dhc@dcrocker.net

DKOR: i=2; mf=dhc@dcrocker.net; rt=dcrocker@gmail.com

A.3. Through a Mailing List

Routed through a mailing list.

DKOR: i=1; mf=brong@fastmailteam.com; rt=ietf-dkim@ietf.org

DKOR: i=2; mf=ietf-dkim@ietf.org.net; rt=dhc@dcrocker.net

A.4. Multiple Mailing Lists

Routed through two mailing lists.

DKOR: i=1; mf=brong@fastmailteam.com; rt=ietf-dkim@ietf.org

DKOR: i=2; mf=ietf-dkim@ietf.org.net; rt=group@example.com

DKOR: i=3; mf=mlm@example.com; rt=dhc@dcrocker.net

A.5. Third-Party Originator

Sent from a third-party service that is originating the message on behalf of someone else. The header fields essentially emulate a kind of mailing list sequence.

DKOR: i=1; mf=esp@example.com; rt=esp@example.com DKOR: i=2; mf=esp@example.com; rt=dhc@dcrocker.net

Acknowledgements

Extended discussions about DKIM Replay converged on the unpleasant necessity to have messages contain only one recipient in the envelope. No alternative approach gained any traction. Further changes produced changes to the draft.

Author’s Address

Dave Crocker
Brandenburg Internetworking
Email: dcrocker@bbiw.net
URI: https://bbiw.net