DMARC
Internet-Draft
Updates: 7489 (if approved)
Intended status: Standards Track
Expires: January 28, 2021

D. Crocker
Brandenburg InternetWorking

July 27, 2020

DMARC Use of the RFC5322.Sender Header Field
draft-crocker-dmarc-sender-01

Abstract

Internet mail defines the RFC5322.From field to indicate the author of the message's content and the RFC5322.Sender field to indicate who initially handled the message. The RFC5322.Sender field is optional, if it has the same information as the RFC5322.From field. That is, when the RFC5322.Sender field is absent, the RFC5322.From field has conflated semantics, with both a handling identifier and a content creator identifier. This was not a problem, until development of stringent protections on use of the RFC5322.From field. It has prompted Mediators, such as mailing lists, to modify the RFC5322.From field, to circumvent mail rejection caused by those protections.

This affects end-to-end behavior of email, between the author and the final recipients, because mail from the same author is not treated the same, depending on what path it followed. In effect, the RFC5322.From field has become dominated by its role as a handling identifier.

The current specification augments use of the RFC5322.From field, by enhancing DMARC to also use the RFC5322.Sender field. This preserves the utility of RFC5322.From field while also preserving the utility of DMARC.

This Internet-Draft will expire on January 28, 2021.

Table of Contents

1. Introduction 2
2. Overview 4
3. Domain Owner Actions 5
4. Mail Originator Actions 5
5. Mail Receiver Actions 6
5.1. Extract RFC5322.Sender and RFC5322.From Domains 6
5.2. Determine Handling Policy 6
6. Security Considerations 7
7. IANA Considerations 7
8. References 7
8.1. Normative References 7
8.2. Informative References 7
Author's Address 8

1. Introduction

Internet mail conducts asynchronous communication from an author to one or more recipients, and is used for ongoing dialogue amongst them. Email has a long history of serving a wide range of human uses and styles, within that simple framework, and the mechanisms for making email robust and safe serve that sole purpose.

Internet mail defines the RFC5322.From field to indicate the author of the message's content and the RFC5322.Sender field to indicate who initially handled the message. [Mail-Fmt] The RFC5322.Sender field is optional, if it has the same information as the RFC5322.From field. That is, when the RFC5322.Sender field is absent, the RFC5322.From field has conflated semantics, as both a handling identifier and a content creator identifier. These fields were

initially defined in [RFC733] and making the redundant RFC5322.Sender field optional was a small, obvious optimization, in the days of slower communications, expensive storage and less powerful computers.

The dual semantics of the RFC5322.From field was not a problem, until development of stringent protections were put in place, on the use of the RFC5322.From field. It has prompted Mediators, such as mailing lists, to modify the RFC5322.From field, to circumvent mail rejection caused by those protections. This affects end-to-end usability of email, between the author and the final recipients. If the mailing list does not modify the RFC5322.From field, there is the risk that the message will be rejected or quarantined by the receiving system. However, if the mailing list does modify the RFC5322.From field, mail received from the same author will be treated differently by the recipient's software, depending on what path the message followed.

By way of example, mail by:

Author Name <user@example.com>

which is sent directly to a recipient, will show the user's display name correctly and can correctly analyze and aggregate mail from that user, based on their email address. However if the user sends through a mailing list, and the mailing list conducts a common form of RFC5322.From modification, needed to bypass enforcement of stringent authentication policies, then the received message might have a RFC5322.From field along the lines of

Author Name via Listname <listname@list.example.com>

The change inserts an operational address, for the Mediator, into the RFC5322.From field, and distorts the field's display-name, as a means of recording the modification. The result is that the recipient's software will see the message as being from an entirely different author and will handle it separately. Mediators might create a Reply-To: field, with the original RFC5322.From field email address. While this facilitates a recipient's responding to the original author, it does nothing to aid other processing done by the recipient's MUA based on what it believes is the author's address or original display-name.

Because the current email protection behavior involves the RFC5322.From field, and pertain to the human author, it is common to think that the issue, in protecting the field's content, is behavior of the human recipient. However there is no indication that the enforced values in the RFC5322.From field alter end-user behavior. In fact there is a long train of indication that it does not. Rather, the meaningful protections actually operate at the level of

the receiving system's mail filtering engine, which decides on the dispostion of received mail.

In effect, the RFC5322.From field has become dominated by its role as a handling identifier. This specification defines enhancement for use of the RFC5322.Sender field by [DMARC]. It is designed with the view that enhancement of standards works best as incremental additions. DMARC functionality is preserved, as is long-standing recipient email usability..

Teminology and architectural details in this document are incorporated from [Mail-Arch].

Discussion of this draft is directed to the dmarc@ietf.org mailing list.

COMMENT: The original version of this specification essentially sought to have the Sender: header field treated as an alternative to the From: header field. Unfortunately this suffers a fatal problem, in the face of established DMARC use.

If:

* the original From: field is covered by DMARC, and

* the message goes through a Mediator that breaks aligned authentication, and

* the receiving DMARC engine only uses the original version of DMARC,

then it will produce a DMARC fail.

It does not appear to be possible to handle this case safely, except by modifying the From: header field so that it does not trigger an alignment failure. Unless there comes a time at which concern for this case is eliminated, Mediators will continue to have to deal with this, such as by modifying the From: field.

To that end, this version of the specification has been modified, to make Sender: an _additional_ DMARC alignment possibility, rather than an alternative one.

2. Overview

This specification defines modifications to DMARC, to add use of the RFC5322.Sender header field, as a possible second source of DMARC validation and policy information. The changes are:

- A tag is added to the DMARC DNS record, to flag support for this enhancement, indicating that valid mail originating from this domain will have an aligned RFC5322.Sender field.

- The message originator creates a RFC5322.Sender field that is identical to the RFC5322.From field, and therefore provides DMARC alignment. This can permit DMARC to validate, even when it fails to validate, based on the From: field.

- Receiving systems supporting the enhancement check for the RFC5322.Sender domain's DNS DMARC record.

  * If there is a record and it contains the enhancement flag, DMARC evaluation is performed on that domain name.

  * If there is no record or the record does not contain the enhancement flag, then DMARC evaluation proceeds is before, using the RFC5322.From domain name.

The enhancement preserves existing DMARC operation, but permits DMARC success in some scenarios that either used to fail or that produce Mediator actions to bypass DMARC. The following table shows DMARC interactions between original vs. enhanced originators and receivers:

\Originate/ || - Receive -->	Original	Enhanced
RFC5322.From	RFC5322.From	RFC5322.From
RFC5322.From + RFC5322.Sender	RFC5322.From	RFC5322.Sender

DMARC Original/Enhanced Interactions

3. Domain Owner Actions

For a domain that supports the use of RFC5322.Sender field evaluation for DMARC, the owner specifies an additional DMARC Policy Record tag:

snd: When present, this tag signals that mail originated by the domain owner MAY have a RFC5322.Sender field, as well as a RFC5322.From field and that evaluation MAY be based on the domain name in the RFC5322.Sender field.

4. Mail Originator Actions

Mail originators, for domains supporting enhanced DMARC, create a RFC5322.Sender field that is a duplicate of the RFC5322.From field.

5. Mail Receiver Actions

5.1. Extract RFC5322.Sender and RFC5322.From Domains

The domain in the RFC5322.Sender field and the domain in the RFC5322.From field are extracted as the domains to be evaluated by DMARC.

5.2. Determine Handling Policy

The following procedure can result in DMARC policy information based on the rfc5322.From, or the rfc5322.Sender, or based on both header fields. The final choice for using this information to determine message disposition resides with the receiving system.

To arrive at a policy for an individual message, Mail Receivers MUST perform the following actions or their semantic equivalents. Steps 2-3 MAY be done in parallel, whereas steps 4 and 5 require input from previous steps.

The steps are as follows:

1.

Sender: Extract the RFC5322.Sender domain from the message.

Query the DNS for a DMARC policy record.

Perform remaining, numbered steps, if one is found and it contains an "snd" tag.

AND

From: Extract the RFC5322.From domain from the message.

Query the DNS for a DMARC policy record

Perform remaining, numbered steps, if one is found.

Terminate: Otherwise terminate DMARC evaluation.

2. Perform DKIM signature verification checks. A single email could contain multiple DKIM signatures. The results of this step are passed to the remainder of the algorithm and MUST include the value of the "d=" tag from each checked DKIM signature.

3. Perform SPF validation checks. The results of this step are passed to the remainder of the algorithm and MUST include the domain name used to complete the SPF check.

4. Conduct Identifier Alignment checks. With authentication checks and policy discovery performed, the Mail Receiver checks to see if Authenticated Identifiers fall into alignment. If one or more of the Authenticated Identifiers align with the RFC5322.From (or with the RFC5322.Sender field, if permitted by the domain owner) domain, the message is considered to pass the DMARC mechanism check. All other conditions (authentication failures, identifier mismatches) are considered to be DMARC mechanism check failures.

5. Apply policy. Emails that fail the DMARC mechanism check are disposed of in accordance with the discovered DMARC policy of the Domain Owner. See Section 6.3 for details.

6. Security Considerations

This enhancement entails the same security issues as the basic DMARC service.

7. IANA Considerations

None.

8. References

8.1. Normative References

[DMARC] Kucherawy, M., Ed. and E. Zwicky, Ed., "Domain-based Message Authentication, Reporting, and Conformance (DMARC)", RFC 7489, March 2015.

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

[Mail-Fmt] Resnick, P., Ed., "Internet Message Format", RFC 5322, October 2008.

8.2. Informative References

[RFC733] Crocker, D., Vittal, J., Pogran, K., and D. Henderson, "Standard for the Format of ARPA Network Text Messages", RFC 733, November 1977.

Author's Address

Dave Crocker
Brandenburg InternetWorking

Email: dcrocker@bbiw.net