The Require-Recipient-Valid-Since Header Field and SMTP Service Extension
draft-ietf-appsawg-rrvs-header-field-06

Abstract

   This document defines an extension for the Simple Mail Transfer
   Protocol called RRVS, and a header field called Require-Recipient-
   Valid-Since, to provide a method for senders to indicate to receivers
   the time when the sender last confirmed the ownership of the target
   mailbox. This can be used to detect changes of mailbox ownership,
   and thus prevent mail from being delivered to the wrong party.

   The intended use of these facilities is on automatically generated
   messages that might contain sensitive information, though it may also
   be useful in other applications.

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 July 14, 2014.

Copyright Notice

Table of Contents

1. Introduction

Email addresses sometimes get reassigned to a different person. For
example, employment changes at a company can cause an address used
for an ex-employee to be assigned to a new employee, or a mail
service provider (MSP) might expire an account and then let someone
else register for the local-part that was previously used. Those who
sent mail to the previous owner of an address might not know that it
has been reassigned. This can lead to the sending of email to the
correct address, but the wrong recipient.

What is needed is a way to indicate an attribute of the recipient
that will distinguish between the previous owner of an address and
its current owner, if they are different. Further, this needs to be
done in a way that respects privacy.

The mechanisms specified here allow the sender of the mail to
indicate how "old" the address assignment is expected to be. In
effect, the sender is saying, "The person to whom I am sending to had
this address assigned to as far back as this date-time." A receiving
system can then compare this information against the date and time
the address was assigned to its current user. If the assignment was
made later than the date-time indicated in the message, there is a
good chance the current user of the address is not the correct
recipient. The receiving system can then choose to prevent delivery
and, possibly, to notify the original sender of the problem.

The primary application is automatically generated messages rather
than user-authored content, though it may be useful in other
contexts.

One important point is that the protocols presented here provide a
way for a sending system to make a request to receiving systems with
respect to handling of a message. In the end, there is no guarantee
that the request will have the desired effect.

2. Definitions

For a description of the email architecture, consult [EMAIL-ARCH].

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

3. Description

To address the problem described above, a mail sending client needs
to indicate to the server to which it is connecting that there is an

   expectation that the destination of the message has been under
   continuous ownership (see Section 10) since some date-time,
   presumably the most recent time the message author had confirmed its
   understanding of who owned that mailbox. Two mechanisms are defined
   here: an extension to the Simple Mail Transfer Protocol [SMTP] and a
   new message header field. The SMTP extension permits strong
   assurance of enforcement by confirming support at each handling step
   for a message. The header field does not provide the strong
   assurance, but only requires adoption by the receiving Message
   Delivery Agent (MDA).

   The SMTP extension is called "RRVS" (Require Recipient Valid Since),
   and adds a parameter to the SMTP "RCPT" command that indicates the
   most recent date and time when the message author believed the
   destination mailbox to be under the continuous ownership of a
   specific party. Similarly, the Require-Recipient-Valid-Since header
   field includes an intended recipient coupled with a timestamp
   indicating the same thing.

3.1. The 'RRVS' SMTP Extension

   Extensions to SMTP are described in Section 2.2 of [SMTP].

   The name of the extension is "RRVS", an abbreviation of "Require
   Recipient Valid Since". Servers implementing the SMTP extension
   advertise an additional EHLO keyword of "RRVS", which has no
   associated parameters, introduces no new SMTP verbs, and does not
   alter the MAIL verb.

   A Message Transfer Agent (MTA) implementing RRVS can transmit or
   accept a new parameter to the RCPT command. An MDA can also accept
   this new parameter. The new parameter is "RRVS", which takes a value
   that is a timestamp expressed as a "date-time" as defined in
   [DATETIME], with the added restriction that a "time-secfrac" MUST NOT
   be used. Accordingly, this extension increases the maximum command
   length for the RCPT verb by 31 characters.

   The meaning of this extension, when used, is described in
   Section 5.1.

3.2. The 'Require-Recipient-Valid-Since' Header Field

   The general constraints on syntax and placement of header fields in a
   message are defined in Internet Message Format [MAIL].

   Using Augmented Backus-Naur Form [ABNF], the syntax for the field is:

      rrvs = "Require-Recipient-Valid-Since:" addr-spec ";" date-time

CRLF

"date-time" is defined in Section 3.3, and "addr-spec" is defined in
Section 3.4.1, of [MAIL].

4. **Use By Generators**

When a message is generated whose content is sufficiently sensitive
that an author or author's Administrative Management Domain (ADMD;
see [EMAIL-ARCH]) wishes to protect against misdelivery using this
protocol, it determines for each recipient mailbox on the message a
timestamp at which it last confirmed ownership of that mailbox. It
then applies either the SMTP extension or the header field defined
above when sending the message to its destination.

Use of the SMTP extension provided here is preferable over the header
field method because of:

1. the positive confirmation of support at each handling node;

2. the fact that the protocol is focused on affecting delivery (that
    is, the transaction) rather than on content; and

3. the fact that there is less risk of the timestamp parameter being
    inadvertently forwarded (see Section 15.3).

The header field mechanism is defined only to enable passage of the
request between and through systems that do not implement the SMTP
extension.

5. **Handling By Receivers**

If a receiver implements this specification, then there are two
possible evaluation paths:

1. The sending client implements the extension, and so there was an
    RRVS parameter on a RCPT TO command in the SMTP session and the
    parameters of interest are taken only from there (and the header
    field, if present, is disregarded); or

2. The sending client does not (or elected not to) implement the
    extension, so the RRVS parameter was not present on the RCPT TO
    commands in the SMTP session, but the corresponding header field
    might be present in the message.

5.1. SMTP Extension Used

   For an MTA supporting the SMTP extension, the requirement is to
   continue enforcement of RRVS during the relaying process to the next
   MTA or the MDA.

   A receiving MDA that implements the SMTP extension declared above and
   observes an RRVS parameter on a RCPT TO command checks whether the
   current owner of the destination mailbox has held it continuously,
   far enough back to include the given date-time, and delivers it
   unless that check returns in the negative. Specifically, an MDA will
   do the following before continuing with delivery:

   1. Ignore the parameter if the named mailbox is known to be a role
       account as listed in Mailbox Names For Common Services, Roles And
       Functions [ROLES]. (See Section 6.)

   2. If the address is not known to be a role account, and if that
       address has not been under continuous ownership since the
       timestamp specified in the extension, return a 550 error to the
       RCPT command. (See also Section 16.3.)

   3. If any Require-Recipient-Valid-Since header fields are present
       and refer to the named address, they SHOULD be removed prior to
       delivery or relaying. (See Section 5.2 and Section 7.1 for
       discussion.)

5.1.1. Relays

   An MTA that does not make mailbox ownership checks, such as an MTA
   positioned to do SMTP ingress at an organizational boundary, SHOULD
   relay the RRVS extension parameter to the next MTA or MDA so that it
   can be processed there.

   See Section 9.2 for additional discussion.

5.2. Header Field Used

   A receiving system that implements this specification, upon receiving
   a message bearing a Require-Recipient-Valid-Since header field when
   no corresponding RRVS SMTP extension was used, checks whether the
   destination mailbox owner has held it continuously, far enough back
   to include the given date-time, and delivers it unless that check
   returns in the negative. Expressed as a sequence of steps:

   1. Extract the set of Require-Recipient-Valid-Since fields from MDA
       the message for which no corresponding RRVS SMTP extension was
       used.

2. Discard any such fields that are syntactically invalid.

3. Discard any such fields that name a role account as listed in
    [ROLES] (see Section 6).

4. Discard any such fields for which the "addr-spec" portion does
    not match a current recipient, as listed in the RCPT TO commands
    in the SMTP session.

5. Discard any such fields for which the "addr-spec" portion does
    not refer to a mailbox handled for local delivery by this ADMD.

6. For each field remaining, determine if the named address has been
    under continuous ownership since the corresponding timestamp. If
    it has not, reject the message.

7. RECOMMENDED: If local delivery is being performed, remove all
    instances of this field prior to delivery to a mailbox; if the
    message is being forwarded, remove those instances of this header
    field that were not discarded by steps 1-4 above.

Handling proceeds normally upon completion of the above steps if
rejection has not been performed.

The final step is not mandatory as not all mail handling agents are
capable of stripping away header fields, and there are sometimes
reasons to keep the field intact such as debugging or presence of
digital signatures that might be invalidated by such a change. See
Section 11 for additional discussion.

If a message is to be rejected within the SMTP protocol itself
(versus generating a rejection message separately), servers
implementing this protocol SHOULD also implement the SMTP extension
described in Enhanced Mail System Status Codes [ESC] and use the
enhanced status codes described in Section 16.3 as appropriate.

Implementation by this method is expected to be transparent to non-
participants, since they would typically ignore this header field.

This header field is not normally added to a message that is
addressed to multiple recipients. The intended use of this field
involves an author seeking to protect transactional or otherwise
sensitive data intended for a single recipient, and thus generating
independent messages for each individual recipient is normal
practice. See Section 8 for further discussion.

[5.2.1](#). Design Choices

The presence of the intended address in the field content supports the case where a message bearing this header field is forwarded. The specific use case is as follows:

1. A user subscribes to a service "S" on date "D" and confirms an email address at the user's current location, "A";

2. At some later date, the user intends to leave the current location, and thus creates a new mailbox elsewhere, at "B";

3. The user replaces address "A" with forwarding to "B";

4. "S" constructs a message to "A" claiming that address was valid at date "D" and sends it to "A";

5. The receiving MTA at "A" determines that the forwarding in effect was created by the same party that owned the mailbox there, and thus concludes the continuous ownership test has been satisfied;

6. If possible, "A" removes this header field from the message, and in either case, forwards it to "B";

7. On receipt at "B", either the header field has been removed, or the header field does not refer to a current envelope recipient, and in either case delivers the message.

SMTP has never required any correspondence between addresses in the [RFC5321](#).MailFrom and [RFC5321](#).RcptTo parameters and header fields of a message, which is why the header field defined here contains the recipient address to which the timestamp applies.

[6](#). Role Accounts

It is necessary not to interfere with delivery of messages to role mailboxes (see [[ROLES](#)]), but it could be useful to notify users sending to those mailboxes that a change of ownership might have taken place, if such notification is possible.

[7](#). Relaying Without RRVS Support

When a message is received using the SMTP extension defined here but will not be delivered locally (that is, it needs to be relayed further), the MTA to which the relay will take place might not be compliant with this specification. Where the MTA in possession of the message observes it is going to relay the message to an MTA that does not advertise this extension, it needs to choose one of the

following actions:

1. Decline to relay the message further, preferably generating a
    Delivery Status Notification [DSN] to indicate failure
    (RECOMMENDED);

2. Downgrade the data thus provided in the SMTP extension to a
    header field, as described in Section 7.1 below (RECOMMENDED when
    the previous option is not available); or

3. Silently continue with delivery, dropping the protection offered
    by this protocol.

Using other than the first option needs to be avoided unless there is
specific knowledge that further relaying with the degraded
protections thus provided does not introduce undue risk.

7.1. Header Field Conversion

If an SMTP server ("B") that has received mailbox timestamps from a
client ("A") using this extension but then needs to relay the
corresponding message on to another server ("C") (thereby becoming a
client), but "C" does not advertise the SMTP extension and "B" elects
not to reject the message, "B" SHOULD add Require-Recipient-Valid-
Since header fields matching each mailbox to which relaying is being
done, and the corresponding valid-since timestamp for each.

Similarly, if "B" receives a message bearing one or more Require-
Recipient-Valid-Since header fields from "A" for which it must now
relay the message, and "C" advertises support for the SMTP extension,
"B" SHOULD delete the header field(s) and instead relay this
information by making use of the SMTP extension. Note that such
modification of the header might affect later validation of the
header upon delivery; for example, a hash of the header would produce
a different result. This might be a valid cause for some operators
to skip this delete operation.

8. Header Field with Multiple Recipients

Numerous issues arise when using the header field form of this
extension, particularly when multiple recipients are specified for a
single message resulting in one multiple fields each with a distinct
address and timestamp.

Because of the nature of SMTP, a message bearing a multiplicity of
Require-Recipient-Valid-Since header fields could result in a single
delivery attempt for multiple recipients (in particular, if two of
the recipients are handled by the same server), and if any one of

them fails the test, the delivery fails to all of them; it then
becomes necessary to do one of the following:

o   reject the message on completion of the DATA phase of the SMTP
    session, which is a rejection of delivery to all recipients; or

o   accept the message on completion of DATA, and then generate a
    Delivery Status Notification [DSN] message for each of the failed
    recipients

Additional complexity arises when a message is sent to two
recipients, "A" and "B", presumably with different timestamps, both
of which are then redirected to a common address "C". The author is
not necessarily aware of the current or past ownership of mailbox
"C", or indeed that "A" and/or "B" have been redirected. This might
result in either or both of the two deliveries failing at "C", which
is likely to confuse the message author, who (as far as the author is
aware) never sent a message to "C" in the first place.

9. Special Use Addresses

In [DSN-SMTP], an SMTP extension was defined to allow SMTP clients to
request generation of DSNs, and related information to allow such
reports to be maximally useful. Section 5.2.7 of that document
explored the issue of the use of that extension where the recipient
is a mailing list. This extension has similar concerns which are
covered here following that document as a model.

9.1. Mailing Lists

Delivery to a mailing list service is considered a final delivery.
Where this protocol is in use, it is evaluated as per any normal
delivery: If the same mailing list has been operating in place of the
specified recipient mailbox since at least the timestamp given as the
RRVS parameter, the message is delivered to the list service
normally, and is otherwise not delivered.

It is important, however, that the participating MDA passing the
message to the list service needs to omit the RRVS parameter in
either form (SMTP extension or header field) when doing so. The
emission of a message from the list service to its subscribers
constitutes a new message not covered by the previous transaction.

9.2. Single-Recipient Aliases

Upon delivery of an RRVS-protected message to an alias (acting in
place of a mailbox) that results in relaying of the message to a
single other destination, the usual RRVS check is performed. The

continuous ownership test here might succeed if a conventional user
inbox was replaced with an alias on behalf of that same user, and
this information is recorded someplace. If the message is thus
accepted, the relaying MTA can choose to do one of the following:

1. Do not include an RRVS parameter or header field when relaying to
    the new address. (RECOMMENDED)

2. If the relaying system records the time when the alias was
    established, independent of confirming the validity of the new
    destination address, it MAY add an RRVS parameter for the new
    target address that includes that time.

3. If an explicit confirmation of the new destination was done, it
    MAY add an RRVS parameter for the new target address that
    includes that time.

There is risk and additional administrative burden associated with
all but the first option in that list which are believed to make them
not worth pursuing.

9.3. Multiple-Recipient Aliases

Upon delivery of an RRVS-protected message to an alias (acting in
place of a mailbox) that results in relaying of the message to
multiple other destinations, the usual RRVS check is performed as in
Section 9.2. The MTA expanding such an alias then decides which of
the options enumerated in that section is to be applied for each new
recipient.

9.4. Confidential Forwarding Addresses

In the above cases, the original author could receive message
rejections, such as DSNs, from the ultimate destination, where the
RRVS check (or indeed, any other) fails and rejection is warranted.
This can reveal the existence of a forwarding relationship between
the original intended recipient and the actual final recipient.

Where this is a concern, the initial delivery attempt is to be
treated like a mailing list delivery, with RRVS evaluation done and
then all RRVS information removed from the message prior to relaying
it to its true destination.

9.5. Suggested Mailing List Enhancements

Mailing list services could store the timestamp at which a subscriber
was added to a mailing list. This specification could then be used
in conjunction with that information in order to restrict list

   traffic to the original subscriber, rather than a different person
   now in possession of an address under which the original subscriber
   was added to the list. Upon receiving a rejection caused by this
   specification, the list service can remove that address from further
   distribution.

   A mailing list service that receives a message containing the header
   field defined here needs to remove it from the message prior to
   redistributing it, limiting exposure of information regarding the
   relationship between the message's author and the mailing list.

10. Continuous Ownership

   For the purposes of this specification, an address is defined as
   having been under continuous ownership since a given date-time if a
   message sent to the address at any point since the given date would
   not go to anyone except the owner at that given date-time. That is,
   while an address may have been suspended or otherwise disabled for
   some period, any mail actually delivered would have been delivered
   exclusively to the same owner. It is is presumed that some sort of
   relationship exists between the message sender and the intended
   recipient. Presumably there has been some confirmation process
   applied to establish this ownership of the receiver's mailbox;
   however, the method of making such determinations is a local matter
   and outside the scope of this document.

   Evaluating the notion of continuous ownership is accomplished by
   doing any query that establishes whether the above condition holds
   for a given mailbox.

   Determining continuous ownership of a mailbox is a local matter at
   the receiving site. The only possible answers to the continuous-
   ownership-since question are "yes", "no", and "unknown"; the action
   to be taken in the "unknown" case is a matter of local policy.

   For example, when control of a domain name is transferred, the new
   domain owner might be unable to determine whether the owner of the
   subject address has been under continuous ownership since the stated
   date if the mailbox history is not also transferred (or was not
   previously maintained). It will also be "unknown" if whatever
   database contains mailbox ownership data is temporarily unavailable
   at the time a message arrives for delivery. In this latter case,
   typical SMTP temporary failure handling is appropriate.

   To further obscure account details on the receiving system, the
   receiver SHOULD ignore the SMTP extension or the header field if the
   address specified has had one continuous owner since it was created,
   regardless of the purported confirmation date of the address. This

is further discussed in Section 14.

11. Digital Signatures

This protocol mandates removal of the header field (when used) upon
delivery in all but iexceptional circumstances. Altering a message
in this way will invalidate a digital signature intended to guard
against message modification in transit, which can interfere with
delivery.

Section 5.4.1 of DomainKeys Identified Mail [DKIM] proposes a
strategy for selecting header fields to sign. Specifically, it
advises including in the signed portion of the message only those
header fields that comprise part of the core content of the message.
As the header field version of this protocol is ephemeral, it cannot
be considered core content.

Accordingly, applying digital signatures that attempt to protect the
content of this header field is NOT RECOMMENDED.

12. Authentication-Results Definitions

[AUTHRES] defines a mechanism for indicating, via a header field, the
results of message authentication checks. Section 16 registers RRVS
as a new method that can be reported in this way, and corresponding
result names. The possible result names and their meanings are as
follows:

none: The message had no recipient mailbox timestamp associated with
   it, either via the SMTP extension or header field method; this
   protocol was not in use.

unknown: At least one form of this protocol was in use, but
   continuous ownership of the recipient mailbox could not be
   determined.

temperror: At least one form of this protocol was in use, but some
   kind of error occurred during evaluation that was transient in
   nature; a later retry will likely produce a final result.

permerror: At least one form of this protocol was in use, but some
   kind of error occurred during evaluation that was not recoverable;
   a later retry will not likely produce a final result.

pass: At least one form of this protocol was in use, and the
   destination mailbox was confirmed to have been under constant
   ownership since the timestamp thus provided.

fail: At least one form of this protocol was in use, and the
   destination mailbox was confirmed not to have been under constant
   ownership since the timestamp thus provided.

Where multiple recipients are present on a message, multiple results
can be reported using the mechanism described in [AUTHRES].

13. Examples

In the following examples, "C:" indicates data sent by an SMTP
client, and "S:" indicates responses by the SMTP server. Message
content is CRLF terminated, though these are omitted here for ease of
reading.

13.1. SMTP Extension Example

```
C: [connection established]
S: 220 server.example.com ESMTP ready
C: EHLO client.example.net
S: 250-server.example.com
S: 250 RRVS
C: MAIL FROM:<sender@example.net>
S: 250 OK
C: RCPT TO:<receiver@example.com> RRVS=1381993177
S: 550 5.7.17 receiver@example.com is no longer valid
C: QUIT
S: 221 So long!
```

13.2. Header Field Example

```
C: [connection established]
S: 220 server.example.com ESMTP ready
C: HELO client.example.net
S: 250 server.example.com
C: MAIL FROM:<sender@example.net>
S: 250 OK
C: RCPT TO:<receiver@example.com>
S: 250 OK
C: DATA
S: 354 Ready for message content
C: From: Mister Sender <sender@example.net>
   To: Miss Receiver <receiver@example.com>
   Subject: Are you still there?
   Date: Fri, 28 Jun 2013 18:01:01 +0200
   Require-Recipient-Valid-Since: receiver@example.com;
     Sat, 1 Jun 2013 09:23:01 -0700

   Are you still there?
   .
S: 550 5.7.17 receiver@example.com is no longer valid
C: QUIT
S: 221 So long!
```

13.3. Authentication-Results Example

An example use of the Authentication-Results header field used to
yield the results of an RRVS evaluation:

```
Authentication-Results: mx.example.com; rrvs=pass
        smtp.rcptto=user@example.com
```

This indicates that the message arrived addressed to the mailbox
user@example.com, the continuous ownership test was applied with the
provided timestamp, and the check revealed that test was satisfied.
The timestamp is not revealed.

14. Security Considerations

14.1. Abuse Countermeasures

The response of a server implementing this protocol can disclose
information about the age of existing email mailbox. Implementation
of countermeasures against probing attacks is advised. For example,
an operator could track appearance of this field with respect to a
particular mailbox and observe the timestamps being submitted for
testing; if it appears a variety of timestamps is being tried against
a single mailbox in short order, the field could be ignored and the
message silently discarded. This concern is discussed further in

Section 15.

14.2. Suggested Use Restrictions

If the mailbox named in the field is known to have had only a single
continuous owner since creation, or not to have existed at all (under
any owner) prior to the date specified in the field, then the field
can be silently ignored and normal message handling applied so that
this information is not disclosed. Such fields are likely the
product of either gross error or an attack.

A message author using this specification might restrict inclusion of
the header field such that it is only done for recipients known also
to implement this specification, in order to reduce the possibility
of revealing information about the relationship between the author
and the mailbox.

If ownership of an entire domain is transferred, the new owner may
not know what addresses were assigned in the past by the prior owner.
Hence, no address can be known not to have had a single owner, or to
have existed (or not) at all. In this case, the "unknown" result is
likely appropriate.

14.3. False Sense of Security

Senders implementing this protocol likely believe their content is
being protected by doing so. It has to be considered, however, that
receiving systems might not implement this protocol correctly, or at
all. Furthermore, use of RRVS by a sending system constitutes
nothing more than a request to the receiving system; that system
could choose not to prevent delivery for some local policy or
operational reason, which compromises the security the sending system
believed was a benefit to using RRVS. This could mean the timestamp
information involved in the protocol becomes inadvertently revealed.

This concern lends further support to the notion that senders would
do well to avoid using this protocol other than when sending to
known, trusted receivers.

15. Privacy Considerations

15.1. Probing Attacks

As described above, use of this extension or header field in probing
attacks can disclose information about the history of the mailbox.
The harm that can be done by leaking any kind of private information
is difficult to predict, so it is prudent to be sensitive to this
sort of disclosure, either inadvertently or in response to probing by

an attacker. It bears restating, then, that implementing
countermeasures to abuse of this capability needs strong
consideration.

That some MSPs allow for expiration of account names when they have
been unused for a protracted period forces a choice between two
potential types of privacy vulnerabilities, one of which presents
significantly greater threats to users than the other. Automatically
generated mail is often used to convey authentication credentials
that can potentially provide access to extremely sensitive
information. Supplying such credentials to the wrong party after a
mailbox ownership change could allow the previous owner's data to be
exposed without his or her authorization or knowledge. In contrast,
the information that may be exposed to a third party via the proposal
in this document is limited to information about the mailbox history.
Given that MSPs have chosen to allow transfers of mailbox ownership
without the prior owner's involvement, the information leakage from
the extensions specified here creates far fewer risks than the
potential for delivering mail to the wrong party.

15.2. Envelope Recipients

The email To and Cc header fields are not required to be populated
with addresses that match the envelope recipient set, and Cc may even
be absent. However, the algorithm in Section 3 requires that this
header field contain a match for an envelope recipient in order to be
actionable. As such, use of this specification can reveal some or
all of the original intended recipient set to any party that can see
the message in transit or upon delivery.

For a message destined to a single recipient, this is unlikely to be
a concern, which is one of the reasons use of this specification on
multi-recipient messages is discouraged.

15.3. Risks with Use of Header Field

MDAs might not implement the recommendation to remove the header
field defined here when messages are delivered, either out of
ignorance or due to error. Since user agents often do not render all
of the header fields present, the message could be forwarded to
another party that would then inadvertently have the content of this
header field.

A bad actor may detect use of either form of the RRVS protocol and
interpret it as an indication of high value content.

16. IANA Considerations

16.1. SMTP Extension Registration

   Section 2.2.2 of [MAIL] sets out the procedure for registering a new
   SMTP extension. IANA is requested to register the SMTP extension
   using the details provided in Section 3.1 of this document.

16.2. Header Field Registration

   IANA is requested to add the following entry to the Permanent Message
   Header Field Names registry, as per the procedure found in
   [IANA-HEADERS]:

     Header field name: Require-Recipient-Valid-Since
     Applicable protocol: mail ([MAIL])
     Status: Standard
     Author/Change controller: IETF
     Specification document(s): [this document]
     Related information:
       Requesting review of any proposed changes and additions to
       this field is recommended.

16.3. Enhanced Status Code Registration

   IANA is requested to register the following in the Enumerated Status
   Codes table of the Simple Mail Transfer Protocol (SMTP) Enhanced
   Status Codes Registry:

     Code: X.7.17
     Sample Text: Mailbox owner has changed
     Associated basic status code: 5
     Description: This status code is returned when a message is
                           received with a Require-Recipient-Valid-Since
                           field or RRVS extension and the receiving
                           system is able to determine that the intended
                           recipient mailbox has not been under
                           continuous ownership since the specified date.
     Reference: [this document]
     Submitter: M. Kucherawy
     Change controller: IESG

          Code: X.7.18
          Sample Text: Domain owner has changed
          Associated basic status code: 5
          Description: This status code is returned when a message is
                               received with a Require-Recipient-Valid-Since
                               field or RRVS extension and the receiving
                               system wishes to disclose that the owner of
                               the domain name of the recipient has changed
                               since the specified date.
          Reference: [this document]
          Submitter: M. Kucherawy
          Change controller: IESG

16.4. Authentication Results Registration

   IANA is requested to register the following in the "Email
   Authentication Methods" Registry:

   Method: rrvs

   Specifying Document: [this document]

   ptype: smtp

   Property: rcptto

   Value: envelope recipient

   Status: active

   Version: 1

   IANA is also requested to register the following in the "Email
   Authentication Result Names" Registry:

   Codes: none, unknown, temperror, permerror, pass, fail

   Defined: [this document]

   Auth Method(s): rrvs

   Meaning: Section 12 of [this document]

   Status: active

17. References

17.1. Normative References

[ABNF]   Crocker, D., Ed. and P. Overell, "Augmented BNF for
                Syntax Specifications: ABNF", RFC 5234, January 2008.

[DATETIME]   Klyne, G. and C. Newman, "Date and Time on the
                Internet: Timestamps", RFC 3339, July 2002.

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

[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.

[ROLES]   Crocker, D., "Mailbox Names For Common Services,
                Roles And Functions", RFC 2142, May 1997.

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

17.2. Informative References

[AUTHRES]   Kucherawy, M., "Message Header Field for Indicating
                Message Authentication Status", RFC 7001,
                September 2013.

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

[DSN]   Moore, K. and G. Vaudreuil, "An Extensible Message
                Format for Delivery Status Notifications", RFC 3464,
                January 2003.

[DSN-SMTP]   Moore, K., "Simple Mail Transfer Protocol (SMTP)
                Service Extension for Delivery Status Notifications
                (DSNs)", RFC 3461, January 2003.

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

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

Appendix A. Acknowledgments

Erling Ellingsen proposed the idea.

Reviews and comments were provided by Michael Adkins, Kurt Andersen, Eric Burger, Alissa Cooper, Dave Cridland, Dave Crocker, Ned Freed, John Levine, Alexey Melnikov, Hector Santos, Gregg Stefancik, Ed Zayas, (others)

Authors' Addresses

William J. Mills
Yahoo! Inc.

EMail: wmills_92105@yahoo.com

Murray S. Kucherawy
Facebook, Inc.
1 Hacker Way
Menlo Park, CA 94025
USA

EMail: msk@fb.com