Network Working Group   W. Mills
Internet-Draft   Yahoo! Inc.
Intended status: Standards Track   M. Kucherawy
Expires: October 18, 2014   Facebook, Inc.
                                                      April 16, 2014

**The Require-Recipient-Valid-Since Header Field and SMTP Service
Extension**
draft-ietf-appsawg-rrvs-header-field-10

Abstract

   This document defines an extension for the Simple Mail Transfer
   Protocol called RRVS, to provide a method for senders to indicate to
   receivers a point in time when the the ownership of the target
   mailbox was known to the sender. This can be used to detect changes
   of mailbox ownership, and thus prevent mail from being delivered to
   the wrong party. This document also defines a header field called
   Require-Recipient-Valid-Since that can be used to tunnel the request
   through servers that do not support the extension.

   The intended use of these facilities is on automatically generated
   messages, such as account statements or password change instructions,
   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 October 18, 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. This situation is of
particular concern with transactional mail related to purchases,
online accounts, and the like.

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, "I know that the intended recipient was
using this address at this point in time. I don't want this message
delivered to anyone else" A receiving system can then compare this
information against the point in time at which the address was
assigned to its current user. If the assignment was made later than
the point in 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 prevent delivery and, preferably, notify
the original sender of the problem.

The primary application is transactional mail (such as account
information, password change requests, and other automatically
generated messages) rather than user-authored content. However, it
may be useful in other contexts; for example, a personal address book
could record the time an email address was added to it, and thus use
that time with this extension.

Because the use cases for this extension are strongly tied to privacy
issues, attention to the Security Considerations (Section 13) and the
Privacy Considerations (Section 14), is particularly important.
Note, especially, the limitation described in Section 13.3.

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 in Section 1, a mail sending client
(usually an automated agent) needs to indicate to the server to which
it is connecting that it expects the destination address of the
message to have been under continuous ownership (see Section 9) since
a specified point time. That specified time would be the time when
the intended recipient gave the address to the message author, or
perhaps a more recent time when the intended recipient reconfirmed
ownership of the address with the sender.

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, and the option to demand
support at all nodes in the handling path of the message (and
returning of the message to the originator otherwise). The header
field can be used when the Message Delivery Agent (MDA) supports this
function, but an intermediary system between the sending system and
the MDA does not. However, the header field does not provide the
same strong assurance described above, and is more prone to exposure
of private information (see Section 14.1).

The SMTP extension is called "RRVS" (Require Recipient Valid Since),
and adds a parameter to the SMTP "RCPT" command that indicates the
most recent point in 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 commands, and does not
alter the MAIL command.

A Message Transfer Agent (MTA) implementing RRVS can transmit or
accept one new parameter to the RCPT command. An MDA can also accept
this new parameter. The parameter is "RRVS", and the value is a
timestamp expressed as a "date-time" as defined in [DATETIME], with
the added restriction that a "time-secfrac" MUST NOT be used. The

timestamp MAY optionally be followed by a semi-colon character and a
letter (known as the "no-support action") indicating the action to be
taken when a downstream MTA is discovered that does not support the
extension. Valid actions are "R" (reject; the default) and "C"
(continue).

Formally, the new parameter and its value are defined as follows:

```
    rrvs-param = "RRVS=" date-time [ ";" ( "C" / "R" ) ]
```

Accordingly, this extension increases the maximum command length for
the RCPT command by 33 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].

3.3. Timestamps

The header field version of this protocol has a different format for
the date and time expression than the SMTP extension does. This is
because message header fields use a format to express time and date
that is specific to message header fields, and this is consistent
with that usage.

Use of both date and time is done to be consistent with how current
implementations typically store the timestamp, and to make it easy to
include the time zone. In practice, granularity beyond the date may
or may not be useful.

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 the SMTP extension when sending the message to its
destination.

In cases where the outgoing MTA does not support the extension, the
header field defined above can be used to pass the request through
that system. However, use of the header field is only a "best-
effort" approach to solving the stated goals, and it has some
shortcomings:

1. The positive confirmation of support at each handling node, with
    the option to return the message to the originator when end-to-
    end support cannot be confirmed, will be unavailable;

2. The protocol is focused on affecting delivery (that is, the
    transaction) rather than on content, and therefore use of a
    header field in the content is generally inappropriate;

3. The mechanism cannot be used with multiple recipients without
    unintentionally exposing information about one recipient to the
    others (see Section 7; and

4. There is a risk of the timestamp parameter being inadvertently
    forwarded, automatically or intentionally by the user (since user
    agents might not reveal the presence of the header field), and
    therefore exposed to unintended recipients. (See Section 14.4.)

Thus, the header field format MUST NOT be used unless the originator
or relay has specific knowledge that the receiving MDA or an
intermediary MTA will apply it properly. In any case, it SHOULD NOT
be used for the multi-recipient case.

Use of the header field mechanism is further restricted by the
practices described in Section 7.2 of [SMTP], Section 3.6.3 of
[MAIL], and Section 7 of this document.

5. Handling By Receivers

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

1. The sending client uses 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 use 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.

When the continuous ownership test fails for transient reasons (such
as an unavailable database or other condition that is likely
temporary), normal transient failure handling for the message is
applied.

If the continuous ownership test cannot be completed because the
necessary datum (the mailbox creation or reassignment date/time) was
not recorded, the MDA doing the evaluation selects a date and time to
use that is the latest possible point in time at which the mailbox
could have been created or reassigned. For example, this might be
the earliest of all recorded mailbox creation/reassignment
timestamps, or the time when the host was first installed. If no
reasonable substitute for the timestamp can be selected, the MDA
rejects the message using an SMTP reply code, preferably with an
enhanced mail system status code (see Section 15.3), that indicates
the test cannot be completed. A message originator can then decide
whether to reissue the message without RRVS protection, or find
another way to reach the mailbox owner.

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 MTA or 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 point in 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].

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 15.3.)

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.

For the SMTP extension, the optional RRVS parameter defined in
Section 5.1 indicates the action to be taken when relaying a message
to another MTA that does not advertise support for this extension.
When this is the case and the no-support action was not specified or
is "R" (reject), the MTA handling the message MUST reject the message
by:

1. returning a 550 error to the DATA command, if synchronous service
    is being provided to the SMTP client that introduced the message;
    or

2. generating a [DSN] to indicate to the originator of the message
    that the non-delivery occurred, and terminating further relay
    attempts.

An enhanced mail system status code is defined for such rejections in
Section 15.3.

See Section 8.2 for additional discussion.

When relaying, an MTA MUST preserve the no-support action if it was
used by the SMTP client.

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 those Require-Recipient-Valid-Since fields from the
    message that contain a recipient for which no corresponding RRVS
    SMTP extension was used.

2. Discard any such fields that match any of these criteria:

    * are syntactically invalid;

> * name a role account as listed in [ROLES];
>
> * the "addr-spec" portion does not match a current recipient, as
>   listed in the RCPT TO commands in the SMTP session; or
>
> * the "addr-spec" portion does not refer to a mailbox handled
>   for local delivery by this ADMD.

3. 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.

4. 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 step 2 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 10 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 15.3 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 7 for further discussion and restrictions.

5.2.1. Design Choices

The presence of the 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 configures address "A" to forward 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 for "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, the MTA for "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.

   Section 8 discusses some interesting use cases, such as the case
   where "B" above results in further forwarding of 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.

5.3. Clock Synchronization

   The timestamp portion of this specification supports a precision at
   the seconds level. Although uncommon, it is not impossible for a
   clock at either a generator or a receiver to be incorrect, leading to
   an incorrect result in the RRVS evaluation.

   To minimize the risk of such incorrect results, both generators and
   receivers implementing this specification MUST use a standard clock
   synchronization protocol such as [NTP] to synchronize to a common
   clock.

6. 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 6.1 below (SHOULD NOT
    unless the conditions in that section are satisfied, and only
    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.

6.1. Header Field Conversion

If an SMTP server ("B") receives a message bearing one or more
Require-Recipient-Valid-Since from a client ("A"), presumably because
"A" does not support the SMTP extension, and needs to relay the
corresponding message on to another server ("C") (thereby becoming a
client), 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 modified header would produce a different
result. This might be a valid cause for some operators to skip this
delete operation.

Conversely, if "B" has received a mailbox timestamp from "A" using
the SMTP extension for which it must now relay the message on to "C",
but "C" does not advertise the SMTP extension, and "B" does not
reject the message because rejection was specifically declined by the
client (see Section 5.1.1), "B" SHOULD add a Require-Recipient-Valid-
Since header field matching the mailbox to which relaying is being
done, and the corresponding valid-since timestamp for it, if it has
prior information that the eventual MDA or another intermediate MTA
supports this mechanism and will be able to process the header field
as described in this specification.

The admonitions about very cautious use of the header field described
in Section 4 apply to this relaying mechanism as well. If multiple

mailbox timestamps are received from "A", the admonitions in
Section 7 also apply.

7. 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 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.

Finally, there is an obvious concern with the fan-out of a message
bearing the timestamps of multiple users; tight control over the
handling of the timestamp information is very difficult to assure as
the number of handling agents increases.

8. 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.

For all cases described below, a receiving MTA SHOULD NOT introduce

RRVS in either form (SMTP extension or header field) if the message
did not arrive with RRVS in use. This would amount to second-
guessing of the message originator's intention and might lead to an
undesirable outcome.

8.1. 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.

8.2. 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, for example, a
conventional user inbox was replaced with an alias on behalf of that
same user, and the time when this was done is recorded in a way that
can be queried by the relaying MTA.

If the relaying system also performs some kind of step where
ownership of the new destination address is confirmed, it SHOULD
apply RRVS using the later of that timestamp and the one that was
used inbound. This also allows for changes to the alias without
disrupting the protection offered by RRVS.

If the relaying system has no such time records related to the new
destination address, the RRVS SMTP extension is not used on the
relaying SMTP session, and the header field relative to the local
alias is removed, in accordance with Section 5.

8.3. 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 8.2. The MTA expanding such an alias then decides which of
the options enumerated in that section is to be applied for each new

recipient.

8.4. 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.

8.5. 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.

9. 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 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 avoid exposing account details unnecessarily, if the address
   specified has had one continuous owner since it was created, any
   confirmation date SHOULD be considered to pass the test, even if that
   date is earlier than the account creation date. This is further
   discussed in Section 13.

10. Digital Signatures

   This protocol mandates removal of the header field (when used) upon
   delivery in all but exceptional circumstances. If a message with the
   header field were digitally signed in a way that included the header
   field, altering a message in this way would invalidate the signature.
   However, the header field is strictly for tunneling purposes and
   should be regarded by the rest of the transport system as purely
   trace information.

   Accordingly, the header field MUST NOT be included in the content
   covered by digital signatures.

11. Authentication-Results Definitions

   [AUTHRES] defines a mechanism for indicating, via a header field, the
   results of message authentication checks. Section 15 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 continuous
     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
     continuous 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].

12. 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.

12.1. 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=2014-04-03T23:01:00Z
S: 550 5.7.17 receiver@example.com is no longer valid
C: QUIT
S: 221 So long!
```

12.2. **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!
```

12.3. **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.

13. **Security Considerations**

13.1. **Abuse Countermeasures**

   The response of a server implementing this protocol can disclose
   information about the age of an existing email mailbox.
   Implementation of countermeasures against probing attacks is
   RECOMMENDED. 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 14.

13.2. 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
SHOULD 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.

13.3. 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, legal 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.

13.4. Reassignment of Mailboxes

This specification is a direct response to the risks involved with
reassignment or recycling of email addresses, an inherently dangerous
practice. It is typically expected that email addresses will not
have a high rate of turnover or ownership change.

It is RECOMMENDED to have a substantial period of time between
mailbox owners during which the mailbox accepts no mail, giving
message generators an opportunity to detect that the previous owner
is no longer at that address.

14. Privacy Considerations

14.1. The Trade-Off

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 lower overall risk than the
potential for delivering mail to the wrong party.

14.2. 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.

14.3. 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.

14.4. Risks with Use

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.

15. IANA Considerations

15.1. 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.

15.2. 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.

15.3. 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


      Code:                 X.7.19
      Sample Text:          RRVS test cannot be completed
      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 cannot complete the requested
                            evaluation because the required timestamp was
                            not recorded.  The message originator needs to
                            decide whether to reissue the message without
                            RRVS protection.
      Reference:            [this document]
      Submitter:            M. Kucherawy
      Change controller:    IESG
```

15.4. 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 11 of [this document]

Status: active

16. References

16.1. 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.

[NTP]   Mills, D., Martin, J., Ed., Burbank, J., and W.

                          Kasch, "Network Time Protocol Version 4: Protocol and
                          Algorithms Specification", RFC 5905, June 2010.

    [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.

16.2. Informative References

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

    [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, Jay Nancarrow, 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