Message Header Field for Indicating Message Authentication Status
draft-kucherawy-sender-auth-header-09

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79. This document may not be modified, and derivative works of it may not be created.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on May 8, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).
Abstract

This memo defines a new message header field for use with electronic mail messages to indicate the results of message authentication efforts. Mail user agents (MUAs) may use this message header field to relay that information in a convenient way to users or to make sorting and filtering decisions.
# Table of Contents

1. Introduction ................................................. 4  
   1.1. Purpose .............................................. 4  
   1.2. Requirements ......................................... 4  
   1.3. Definitions ........................................... 5  
2. Definition and Format of the Header .......................... 6  
   2.1. General Description ................................... 6  
   2.2. Formal Definition ..................................... 6  
   2.3. Authentication Identifier Fields ....................... 8  
   2.4. Result Values .......................................... 9  
   2.5. Definition Of Initial Methods ......................... 10  
   2.6. Extension Fields ..................................... 10  
3. The ‘iprev’ Authentication Method ............................ 11  
4. Adding The Header Field To A Message ......................... 12  
   4.1. Header Position and Interpretation .................... 12  
5. Removing The Header Field .................................. 14  
6. Conformance and Usage Requirements .......................... 15  
7. IANA Considerations ......................................... 16  
   7.1. The Authentication-Results: header .................... 16  
   7.2. Email Authentication Method Name Registry ............. 16  
8. Security Considerations ..................................... 18  
   8.1. Forged Headers ........................................ 18  
   8.2. Misleading Results ................................... 18  
   8.3. Other Protocols ....................................... 19  
   8.4. Header Position ....................................... 19  
9. References .................................................. 20  
   9.1. Normative References .................................. 20  
   9.2. Informative References ................................ 20  
Appendix A. Acknowledgements .................................. 22  
Appendix B. Legacy MUAs ....................................... 23  
Appendix C. Authentication-Results Examples .................... 24  
   C.1. Trivial case; header field not present ................ 24  
   C.2. Nearly-trivial case; service provided, but no authentication done .......................... 25  
   C.3. Service provided, authentication done .................. 25  
   C.4. Service provided, several authentications done, single MTA .................................. 26  
   C.5. Service provided, several authentications done, different MTAs ............................ 27  
   C.6. Service provided, multi-tiered authentication done ... 29  
Appendix D. Public Discussion .................................. 31  
Author’s Address ............................................... 32  
Intellectual Property and Copyright Statements .................. 33
1. Introduction

This memo defines a new message header field for electronic mail messages which presents the results of a message authentication effort in a machine-readable format. The intent is to create a place to collect such data when message authentication mechanisms are in use so that a Mail User Agent (MUA) can provide a recommendation to the user as to the trustworthiness of the message’s origin and content.

This memo defines both the format of this new header field, and discusses the implications of its presence or absence.

[UPDATE PRIOR TO FINAL VERSION] At the time of publication of this draft, [AUTH], [DKIM], [DOMAINKEYS], [SENDERID] and [SPF] are the published e-mail authentication methods in common use. As various methods emerge, it is necessary to prepare for their appearance and encourage convergence in the area of interfacing these filters to MUAs.

Although [SPF] defined a header field called Received-SPF for this purpose, that header field is specific to the conveyance of SPF results only and thus is insufficient to satisfy the requirements enumerated below.

1.1. Purpose

The header field defined in this memo is expected to serve several purposes:

1. Convey to MUAs from filters and Mail Transfer Agents (MTAs) the results of various message authentication checks being applied;

2. Provide a common location for the presentation of this data;

3. Create an extensible framework for specifying new authentication methods as such emerge;

4. Convey the results of message authentication tests to later filtering agents within the same "trust domain", as such agents might apply more or less stringent checks based on message authentication results.

1.2. Requirements

This memo establishes no new requirements on existing protocols or servers, as there is currently no standard place for the described data to be collected or presented.
1.3. Definitions

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 RFC2119.

A "border MTA" is an MTA which acts as a gateway between the general Internet and the users within an organizational boundary.

A "delivery MTA" (or Mail Delivery Agent or MDA) is an MTA which actually enacts delivery of a message to a user’s inbox or other final delivery.

An "intermediate MTA" is an MTA which handles messages after a border MTAs and before a delivery MTA.

Generally it is assumed that the work of applying message authentication schemes takes place at a border MTA or a delivery MTA. This specification is written with that assumption in mind. However, there are some sites at which the entire mail infrastructure consists of a single host. In such cases, such terms as "border MTA" and "delivery MTA" may well apply to the same machine or even the very same agent. It is also possible that message authentication could take place on an intermediate MTA. Although this document doesn’t specifically include such cases, they are not meant to be excluded from this specification.

See [I-D.DRAFT-CROCKER-EMAIL-ARCH] for further discussion on e-mail system architecture.
2. Definition and Format of the Header

This section gives a general overview of the format of the header field being defined, and then provides more formal specification.

2.1. General Description

The new header field being defined here is called "Authentication-Results". It is a Structured Header Field as defined in [MAIL] and thus all of the related definitions in that document apply.

This new header field MUST be added at the top of the message as it transits MTAs which do authentication checks so some idea of how far away the checks were done can be inferred. It therefore should be treated as a Trace Header Field as defined in [MAIL] and thus all of the related definitions in that document apply.

The value of the header field (after removing [MAIL] comments) consists of an authentication identifier and then a series of "method=result" statements indicating which authentication method(s) were applied and their respective results, and then, for each applied method, a "property=value" statement indicating which message property was evaluated.

The header field MAY appear more than once in a single message, or more than one result MAY be represented in a single header field, or a combination of these MAY be applied.

2.2. Formal Definition

Formally, the header field is specified as follows:

header = "Authentication-Results:" [CFWS] authserv-id
        [CFWS] [version] *(";" methodspec *propspec [CFWS])

authserv-id = dot-atom-text
; see below for a description of this element;
; "dot-atom-text" is defined in section 3.2.4 of [MAIL]

version = "version=1*DIGIT [CFWS]
; indicates which version of this specification is in use;
; this draft is version "1"

methodspec = [CFWS] method [CFWS] "=" [CFWS] result
; indicates which authentication method was evaluated
; an indication of which properties of the message
; were evaluated by the authentication scheme being
; applied to yield the reported result

method = token [ "/" version ]
; a method indicates which method’s result is
; represented by "value", and is one of the methods
; explicitly defined as valid in this document
; or is an extension method as defined below

version = 1*( ALPHA / DIGIT ) 0*( "." 1*( ALPHA / DIGIT ) )
; indicates which version of the method was applied

result = "pass" / "hardfail" / "softfail" / "neutral" / "tempererror" / "permerror"
; an indication of the results of the attempt to
; authenticate the message

ptype = "smtp" / "header" / "body" / "policy"
; indicates whether the property being evaluated was
; a parameter to an [SMTP] command, or was a value taken
; from a message header field, or was some property of
; the message body, or some other property evaluated by
; the receiving MTA

property = token
; if "ptype" is "smtp", this indicates which [SMTP]
; command provided the value which was evaluated by the
; authentication scheme being applied; if "ptype" is
; "header", this indicates from which header field the
; value being evaluated was extracted; if "ptype" is
; "body", this indicates the offset into the body at which
; content of interest was detected; if "ptype" is "policy"
; then this indicates the name of the policy which caused
; this header field to be added (see below)

value = [CFWS] token [CFWS] / mailbox
; the value extracted from the message property defined
; by the "ptype.property" construction; if the value
; identifies a mailbox, then it is a "mailbox"
; as defined in section 3.4 of [MAIL];
The "token" is as defined in section 5.1 of [MIME].

See Section 2.3 for a description of the "authserv-id" element.

The list of commands eligible for use with the "smtp" ptype can be found in [SMTP] and subsequent amendments.

"CFWS" is as defined in section 3.2.3 of [MAIL].

The "propspec" may be omitted if for example the method was unable to extract any properties to do its evaluation yet has a result to report.

The "ptype" and "property" values used by each authentication method should be defined in the specification for that method (or its amendments).

The "ptype" and "property" are case-insensitive.

A "ptype" value of "policy" indicates a policy decision about the message not specific to a property of the message that could be extracted. For example, if a method would normally report a "ptype.property" of "header.From" and no From: header field was present, the method can use "policy" to indicate that no conclusion about the authenticity of the message could be reached.

If the parsed "ptype.property" construction clearly identifies a mailbox (in particular, smtp.mail, smtp.rcpt, header.from, header.sender), then the "value" MUST be a "mailbox". Other properties (e.g. smtp.helo) may be evaluated, but the property MUST still be expressed as a "token" for simplified parsing.

### 2.3. Authentication Identifier Fields

Every Authentication-Results header field has an authentication identifier field ("authserv-id" above) which is a single result identifier. This is similar in syntax to a fully-qualified domain name.

The authentication identifier field provides a unique identifier that refers to the authenticating service within a given mail administrative domain. The uniqueness of the identifier is guaranteed by the mail administrative domain that generates it and must pertain to exactly that one mail administrative domain. This identifier is intended to be machine-readable and not necessarily meaningful to users. MUAs may use this identifier to determine...
whether or not the data contained in an Authentication-Results header field can be trusted.

For tracing and debugging purposes, the authentication identifier SHOULD be the domain name of the MTA performing the authentication check whose result is being reported.

Examples of valid authentication identifiers are mail.example.org, engineering.example.net and msl.newyork.example.com.

2.4. Result Values

The six possible values of the "result" are:

pass: The message passed the authentication tests. (This may require accessing an authentication policy of some kind published by the sending domain.)

hardfail: The message failed the authentication tests. (This may require accessing an authentication policy of some kind published by the sending domain.)

softfail: The message failed the authentication tests, and the authentication method has either an explicit (published by the sending domain) or implicit policy, but the policy being used doesn’t require successful authentication of all messages from that domain.

neutral: The authentication method completed without errors, but was unable to reach either a positive or negative result about the message.

temprerror: A temporary (recoverable) error occurred attempting to authenticate the message; either the process couldn’t be completed locally, or (for methods requiring a policy to be accessed) there was a temporary failure retrieving the sending domain’s policy. A later retry may produce a more final result.

permerror: A permanent (unrecoverable) error occurred attempting to authenticate the message; either the process couldn’t be completed locally, or (for methods requiring a policy to be accessed) there was a permanent failure retrieving the sending domain’s policy. A later retry is unlikely to yield a final result.

New methods not specified in this document MUST indicate which of these should be returned when exceptions such as syntax errors are detected.
2.5. Definition Of Initial Methods

As they are currently existing specifications for message authentication, it is appropriate to define an authentication method identifier for each of [AUTH], [DKIM], [DOMAINKEYS], [SENDERID] and [SPF]. Therefore, the authentication method identifiers "auth", "dkim", "domainkeys", "senderid" and "spf" respectively are hereby defined for MTAs applying those specifications for e-mail message authentication. See Section 7 for details.

2.6. Extension Fields

Additional authentication method identifiers may be defined in the future by later revisions or extensions to this specification. Extension identifiers beginning with "x-" will never be defined as standard fields; such names are reserved for experimental use. Method identifiers NOT beginning with "x-" MUST be registered with the Internet Assigned Numbers Authority (IANA) and published in an RFC. See Section 7 for further details.

Extension identifiers may be defined for the following reasons:

1. To allow additional information from emergent authentication systems to be communicated to MUAs. The names of such identifiers should reflect the name of the method being defined, but should not be needlessly long.

2. To allow the creation of "sub-identifiers" which indicate different levels of authentication and differentiate between their relative strengths, e.g. "auth1-weak" and "auth1-strong".

Authentication method implementors are encouraged to provide adequate information, via [MAIL] comments if necessary, to allow an MUA developer to understand or relay ancilliary details of authentication results. For example, if it might be of interest to relay what data was used to perform an evaluation, such information could be relayed as a comment in the header field, such as:

```
Authentication-Results: mx.example.com; foo=pass bar.baz=blob (2 of 3 tests OK)
```
3. The 'iprev' Authentication Method

This section defines an authentication method called "iprev".

"iprev" is an attempt to verify that a client appears to be valid based on some DNS queries. In particular, upon receiving a session initiation of some kind from a client, the IP address of the client peer is queried for matching names (i.e. a number-to-name translation, also known as a "reverse lookup" or a "PTR" record query). Once that result is acquired, a lookup of each of the names (i.e. a name-to-number translation, or an "A" record query) thus retrieved is done. The response to this second check should result in at least one mapping to the client’s IP address.

A successful test using this algorithm constitutes a result of "pass" since the domain in which the client’s PTR claims it belongs has confirmed that claim. A failure to match constitutes a "hardfail". There is no case in which "softfail" or "neutral" can be returned. The remaining "temerror" and "pererror" cases refer respectively to temporary and permanent DNS query errors.
4. Adding The Header Field To A Message

This specification makes no attempt to evaluate the relative strengths of various message authentication methods that may become available. As such, the order of the presented authentication methods and results MUST NOT be used to determine the importance or strength of any given method over another. Instead, the MUA must interpret the result of each method based on its knowledge of what that method evaluates.

The "method" MUST refer to an authentication method declared in the IANA registry, or an extension method as defined in Section 2.6. See Section 7 for further information about the registered methods.

An MTA compliant with this specification MUST add this header field (after performing one or more message authentication tests) to indicate at which host which the test was done, which test got applied and what the result was. If an MTA applies more than one such test, it MUST either add this header field once per test, or one header field indicating all of the results. An MTA MUST NOT add a result to an existing header.

An MTA MAY add this header field containing only the authentication identifier portion to indicate explicitly that no message authentication schemes were applied prior to delivery of this message.

4.1. Header Position and Interpretation

In order to ensure non-ambiguous results and avoid the impact of false header fields, an MUA SHOULD NOT interpret this header field unless specifically instructed to do so by the user. That is, this interpretation should not be "on by default". Naturally then, users would not activate such a feature unless they are certain the header field will be added by the receiving MTA that accepts the mail that is ultimately read by the MUA, and instances of the header field appearing to be from within the trust domain but actually added by foreign MTAs will be removed before delivery.

Furthermore, an MUA SHOULD NOT interpret this header field unless the authentication identifier it bears appears to be one within its own trust domain as configured by the user.

An MUA MUST ignore any result reported using a "result" not specified in this document, or a "ptype" not listed in the corresponding registry for such values as defined in Section 7.

An MUA should not reveal these results to end users unless the
results are accompanied by, at a minimum, some associated reputation data about the message that was authenticated.

As stated in Section 2.1, this header field SHOULD be treated as though it were a trace header field as defined in section 3.6 of [MAIL], and hence MUST not be reordered and MUST be prepended to the message, so that there is generally some indication upon delivery of where in the chain of handling MTAs the message authentication was done.

Further discussion of this can be found in the Section 8 below.
5. Removing The Header Field

For security reasons, a border MTA conforming to this specification MUST delete any discovered instance of this header field which claims to have been added within its trust boundary. For example, a border MTA for example.com receiving a message from outside of its mail domain MUST delete any instance of this header field bearing an authentication identifier indicating the header field was added within example.com prior to adding its own header fields. However, care must be taken not to remove header fields added on messages that remain entirely within the originator’s trust boundary (e.g. local-to-local mail).

Furthermore, a border MTA MAY elect simply to remove all instances of this header field on mail crossing its trust into its trust boundary.

A formal definition of "trust boundary" is deliberately not made here. It is entirely possible that a border MTA for example.com might explicitly trust authentication results asserted by upstream host example.net even though they exist in completely disjoint administrative boundaries. In that case the border MTA MAY elect not to delete those results; moreover, the upstream host doing some authentication work could apply a signing technology such as [DKIM] on its own results to assure downstream hosts of their authenticity. An example of this is provided in Appendix C.

Similarly, in the case of messages signed using [DKIM] or other message signing methods that sign headers, this may invalidate one or more signature on the message if they included the header field to be removed at the time of signing. This behaviour can be desirable since there’s little value in validating the signature on a message with forged headers. However, signing agents MAY therefore elect to omit these header fields from signing to avoid this situation.
6. Conformance and Usage Requirements

An MTA or gateway conforms to this specification if it applies one or more message authentication mechanisms and inserts a header field corresponding to this specification after doing so and prior to delivery (per Section 4) and removes apparently improper headers (per Section 5).

MTAs that are relaying mail rather than delivering it, i.e. are not part of an intended recipient’s trust boundary, MAY perform message authentication or even take actions based on the results found, but SHOULD NOT add an "Authentication-Results" header field if relaying (rather than rejecting or discarding at the gateway). Conversely, an MTA doing local delivery and some form of message authentication MUST add this header field prior to delivery the message in order to be compliant. An exception to the former case is described in Section 5.

A minimal implementation that does at least one message authentication check will add the header field defined by this memo prior to invoking local delivery procedures.

This specification places no restrictions on the processing of the header field’s contents by user agents or distribution lists. It is presented to those packages solely for their own information.
7. IANA Considerations

IANA is requested to register a new header field and to create a new table as described below.

7.1. The Authentication-Results: header

Per [IANA-HEADERS], the "Authentication-Results:" header field is added to the IANA Permanent Message Header Field Registry. The following is the registration template:

- Header field name: Authentication-Results
- Applicable protocol: mail ([RFC2822])
- Status: Standard
- Author/Change controller: IETF
- Specification document(s): [TBD]
- Related information:
  - Requesting review of any proposed changes and additions to this field is recommended.

7.2. Email Authentication Method Name Registry

Names of message authentication methods supported by this specification must be registered with IANA, with the exception of experimental names as described in Section 2.6.

New entries are assigned only for values that have been documented in a published RFC that has IETF Consensus, per [IANA-CONSIDERATIONS]. Each method must register a name, the specification that defines it, one or more "ptype" values appropriate for use with that method, and which "property" value(s) should be reported by that method.

The initial set of entries in this registry is as follows:
| Method   | defined | ptype | property       | value                      |
|----------|---------|-------|----------------+----------------------------|
| auth     | RFC2554 | smtp  | auth           | authenticated user         |
| dkim     | RFC4871 | header| d              | signature "d" tag          |
|          |         |       | i              | value of signature "i" tag |
| dkim-ssp | [TBD]   | header| from           | value of From header field |
|          |         |       |                | w/comments removed         |
| domainkeys | RFC4870 | header| from           | value of From header field |
|          |         |       |                | w/comments removed         |
|          |         |       | sender         | value of Sender header field |
|          |         |       |                | w/comments removed         |
| iprev    | this    | policy| iprev          | client IP address          |
|          | document|       |                |                            |
| senderid | RFC4406 | header| name of header | value of header field used by PRA |
|          |         |       | field used by | w/comments removed         |
|          |         | smtp  | from           | envelope sender            |
| spf      | RFC4408 | smtp  | from           | envelope sender            |
|          |         |       |                |                             |
|          |         | smtp  | helo           | HELO parameter             |
|          |         | smtp  | ehlo           | EHHLO parameter            |
8. Security Considerations

The following security considerations apply when applying or processing the "Authentication-Results" header field:

8.1. Forged Headers

An MUA that accesses a mailbox whose mail is handled by a non-conformant MTA, and understands Authentication-Results header fields, could potentially make false conclusions based on forged header fields. A malicious user or agent could forge a header field using the destination MX for a receiving domain as the hostname token in the value of the header, and with the rest of the value claim that the message was properly authenticated. The non-conformant MTA would fail to strip the forged header field, and the MUA could inappropriately trust it.

It is for this reason an MUA should not have processing of the "Authentication-Results" header field enabled by default; instead it should be ignored, at least for the purposes of enacting filtering decisions, unless specifically enabled by the user after verifying that the MTA is compliant. It is acceptable to have an MUA aware of this specification, but have an explicit list of hostnames whose "Authentication-Results" header fields are trustworthy; however, this list should initially be empty.

Proposed alternate solutions to this problem are nascent. Possibly the simplest is a digital signature on the header field that can be verified by a posted public key. Another would be a means to interrogate the MTA that added the header field to see if it is actually providing any message authentication services and saw the message in question, but this isn’t especially palatable. In either case, a method needs to exist to verify that the host that appears to have added the header field (a) actually did so, and (b) is legitimately adding that header field for this delivery.

8.2. Misleading Results

Until some form of service for querying the reputation of a sending agent is widely deployed, the existence of this header field indicating a "pass" does not render the message trustworthy. It is possible for an arriving piece of spam or other undesirable mail to pass checks by several of the methods enumerated above (e.g. a piece of spam signed using [DKIM] by the originator of the spam). In particular, this issue is not resolved by forged header removal discussed above.

Hence, MUAs must take some care with use of this header even after
possibly malicious headers are scrubbed. There are several potential heuristics that can be used to determine whether an authentication results header is valid. For instance, an MUA could determine after several replies that the user has replied to valid messages. Alternatively, after many messages that contain the same results from diverse paths, the MUA may decide to record that the sender is valid. Similarly, when a different results header field appears, an MUA may decide the older data is no longer trustworthy. In all of these cases prudence dictates that the user be queried in these situations until implementors have had some deployment experience.

8.3. Other Protocols

Mitigation of the forged header attack can also be accomplished by moving the authentication results data into meta-data associated with the message. In particular, an [SMTP] extension could be established which is used to communicate authentication results from the border MTA to intermediate and delivery MTAs; the latter of these could arrange to store the authentication results as meta-data retrieved and rendered along with the message by an [IMAP] client aware of a similar extension in that protocol. The delivery MTA would be told to trust data via this extension only from MTAs it trusts, and border MTAs would not accept data via this extension from any source. There is no vector in such an arrangement for forgery of authentication data by an outside agent.

8.4. Header Position

Despite the requirements of [MAIL], header fields can sometimes be reordered enroute by intermediate MTAs. The goal of requiring header field addition only at the top of a message is an acknowledgement that some MTAs do reorder header fields, but most do not. Thus, in the general case, there will be some indication of which MTAs (if any) handled the message after the addition of the header field defined here.
9. References

9.1. Normative References


9.2. Informative References


Appendix A. Acknowledgements

The author wishes to acknowledge the following for their review and constructive criticism of this proposal: Eric Allman, Mark Delany, Jim Fenton, Tony Hansen, Paul Hoffman, Eliot Lear, John Levine, Miles Libbey, Charles Lindsey, S. Moonesamy, Juan Altmayer Pizzorno, Michael Thomas.
Appendix B. Legacy MUAs

Implementors of this proposal should be aware that many MUAs are unlikely to be retrofit to support the new header field and its semantics. In the interests of convenience and quicker adaptation, a delivery MTA might want to consider adding things that are processed by existing MUAs in addition to the Authentication-Results header field. One suggestion is to include a Priority: header field, on messages that don’t already have such a header field, containing a value that reflects the strength of the authentication that was accomplished, e.g. "low" for weak or no authentication, "normal" or "high" for good or strong authentication.

Some modern MUAs can already filter based on the content of this header field. However, there is keen interest in having MUAs make some kind of graphical representation of this header field’s meaning to end users. Until this capability is added, other interim means of conveying authentication results may be necessary while this proposal and its successors are adopted.
Appendix C.  Authentication-Results Examples

This section presents some examples of the use of this header field to indicate authentication results.

C.1.  Trivial case; header field not present

The trivial case:

Received: from mail-router.example.com
    (mail-router.example.com [192.0.2.1])
    by server.sendmail.com (8.11.6/8.11.6)
    with ESMTP id g1G0r1kA003489;
    Fri, Feb 15 2002 17:19:07 -0800
From: sender@example.com
Date: Fri, Feb 15 2002 16:54:30 -0800
To: receiver@sendmail.com
Message-Id: <12345.abc@example.com>
Subject: here’s a sample

Hello!  Goodbye!

Example 1: Trivial case

The "Authentication-Results" header field is completely absent. The MUA may make no conclusion about the validity of the message. This could be the case because the message authentication services were not available at the time of delivery, or no service is provided, or the MTA is not in compliance with this specification.
C.2. Nearly-trivial case; service provided, but no authentication done

A message that was delivered by an MTA that conforms to this specification but provides no actual message authentication service:

```
Authentication-Results: mail-router.example.com
Received: from mail-router.example.com
            (mail-router.example.com [192.0.2.1])
            by server.sendmail.com (8.11.6/8.11.6)
            with ESMTP id g1G0r1kA003489;
            Fri, Feb 15 2002 17:19:07 -0800
From: sender@example.com
Date: Fri, Feb 15 2002 16:54:30 -0800
To: receiver@sendmail.com
Message-Id: <12345.abc@example.com>
Subject: here’s a sample

Hello! Goodbye!
```

Example 2: Header present but no authentication done

The "Authentication-Results" header field is present, indicating that the delivering MTA (which is named in the value of the header field) conforms to this specification. The absence of any method and result tokens indicates that no message authentication was done.

C.3. Service provided, authentication done

A message that was delivered by an MTA that conforms to this specification and applied some message authentication:

```
Authentication-Results: mail-router.example.com;
            spf=pass smtp.mail=sender@example.com
Received: from dialup-1-2-3-4.example.net
            (dialup-1-2-3-4.example.net [192.0.2.200])
            by mail-router.example.com (8.11.6/8.11.6)
            with ESMTP id g1G0r1kA003489;
            Fri, Feb 15 2002 17:19:07 -0800
From: sender@example.net
Date: Fri, Feb 15 2002 16:54:30 -0800
To: receiver@example.com
Message-Id: <12345.abc@example.net>
Subject: here’s a sample

Hello! Goodbye!
```

Example 3: Header reporting results
The "Authentication-Results" header field is present, indicating that the border MTA (which is identified in the value of the header field) conforms to this specification. Furthermore, the message was authenticated by that MTA via the method specified in [SPF]. The MUA could extract and relay this extra information if desired.

C.4. Service provided, several authentications done, single MTA

A message that was relayed inbound via a single MTA that conforms to this specification and applied three different message authentication checks:

```
Authentication-Results: mail-router.example.com;
    auth=pass (cram-md5) smtp.mail=sender@example.com;
    spf=pass smtp.mail=sender@example.com
Authentication-Results: mail-router.example.com;
    sender-id=pass header.from=sender@example.com
Received: from mail-router.example.com
    (mail-router.example.com [192.0.2.1])
    by dialup-1-2-3-4.example.net (8.11.6/8.11.6)
    with ESMTP id g1G0r1kA003489;
    Fri, Feb 15 2002 17:19:07 -0800
Date: Fri, Feb 15 2002 16:54:30 -0800
To: receiver@example.net
From: sender@example.com
Message-Id: <12345.abc@example.com>
Subject: here’s a sample

Hello!  Goodbye!
```

Example 4: Headers reporting results from one MTA

The "Authentication-Results" header field is present, indicating the delivering MTA (which is identified in the value of the header field) conforms to this specification. Furthermore, the sender authenticated herself/himself to the MTA via a method specified in [AUTH], and both [SPF] and [SENDERID] checks were done and passed. The MUA could extract and relay this extra information if desired.

Two "Authentication-Results" header fields are not required since the same host did all of the checking. The authenticating agent could have consolidated all the results into one header field.

This example illustrates a scenario in which a remote user on a dialup connection (example.net) sends mail to a border MTA (example.com) using SMTP authentication to prove identity. The dialup provider has been explicitly authorized to relay mail as "example.com" resulting in passes by the SPF and SenderID checks.
C.5. Service provided, several authentications done, different MTAs

A message that was relayed inbound by two different MTAs that conform to this specification and applied multiple message authentication checks:

```
Authentication-Results: auth-checker.example.com;
    sender-id=hardfail header.from=sender@example.com;
    dkim=pass (good signature) header.i=sender@example.com
Received: from mail-router.example.com
    (mail-router.example.com [192.0.2.1])
    by auth-checker.example.com (8.11.6/8.11.6)
    with ESMTP id i7PK0sH7021929;
    Fri, Feb 15 2002 17:19:22 -0800
Authentication-Results: mail-router.example.com;
    auth=pass (cram-md5) smtp.mail=sender@example.com;
    spf=hardfail smtp.mail=sender@example.com
Received: from dialup-1-2-3-4.example.net
    (dialup-1-2-3-4.example.net [192.0.2.200])
    by mail-router.example.com (8.11.6/8.11.6)
    with ESMTP id g1G0r1kA003489;
    Fri, Feb 15 2002 17:19:07 -0800
DKIM-Signature: v=1; a=rsa-sha256; s=gatsby; d=example.com;
    t=1188964191; c=simple/simple;
    h=From:Date:To:Message-Id:Subject;
    bh=sEuZGD/pSr7ANysbY3jtdaQ3Xv9xPQtS0m70;
    b=EToRSuvUFQVP3Bkz ... rTB0t0gYnBVCM=
From: sender@example.com
Date: Fri, Feb 15 2002 16:54:30 -0800
To: receiver@sendmail.com
Message-Id: <12345.abc@example.com>
Subject: here's a sample
Hello!  Goodbye!
```

Example 5: Headers reporting results from multiple MTAs

The "Authentication-Results" header field is present, indicating conformance to this specification. It is present twice because two different MTAs in the chain of delivery did authentication tests. The first, "mail-router.example.com" reports that [AUTH] and [SPF] were both used, and [AUTH] passed but [SPF] failed. In the [AUTH] case, additional data is provided in the comment field, which the MUA can choose to render if desired.

The second MTA, identifying itself as "auth-checker.example.com", reports that it did a [SENDERID] test (which failed) and a [DKIM] test (which passed). Again, additional data about one of the tests
is provided as a comment, which the MUA may choose to render.

Since different hosts did the two sets of authentication checks, the header fields cannot be consolidated in this example.

This example illustrates more typical transmission of mail into "example.com" from a user on a dialup connection "example.net". The user appears to be legitimate as he/she had a valid password allowing authentication at the border MTA using [AUTH]. The [SPF] and [SENDERID] tests failed since "example.com" has not granted "example.net" authority to relay mail on its behalf. However, the [DKIM] test passed because the sending user had a private key matching one of "example.com"'s published public keys and used it to sign the message.
C.6. Service provided, multi-tiered authentication done

A message that had authentication done at various stages, one of which was outside the receiving domain:

```
Authentication-Results: chicago.example.com;
dkim=pass (good signature) header.i=@mail-router.example.net;
dkim=hardfail (bad signature) header.i=@newyork.example.com
Received: from mail-router.example.net
              (mail-router.example.net [192.0.2.250])
by chicago.example.com (8.11.6/8.11.6)
          for <recipient@chicago.example.com>
          with ESMTP id i7PK0sH7021929;
         Fri, Feb 15 2002 17:19:22 -0800
DKIM-Signature: v=1; a=rsa-sha256; s=furble;
d=mail-router.example.net; t=1188964198; c=relaxed/simple;
h=From:Date:To:Message-Id:Subject:Authentication-Results;
bh=ftA9J6GtX8opwUECzHnCkRzKw1uk6FNiLfJ15Nmv49E=
     b=oINEO8hgn/gnunsg ... 9n90D6N5Dij3=
Authentication-Results: mail-router.example.net;
dkim=pass (good signature) header.i=@newyork.example.com
Received: from smtp.newyork.example.com
              (smtp.newyork.example.com [192.0.2.220])
by mail-router.example.net (8.11.6/8.11.6)
          with ESMTP id g1G0r1kA003489;
         Fri, Feb 15 2002 17:19:07 -0800
DKIM-Signature: v=1; a=rsa-sha256; s=gatsby;
d=newyork.example.com;
t=1188964191; c=simple/simple;
h=From:Date:To:Message-Id:Subject;
bh=sEu28nfs9fuZGD/pSr7ANysbY3jtdaQ3xv9xPQtS0m7=
     b=ETOtv7uvUFVF3Bkz ... rT80t9gYnBVCM=
From: sender@newyork.example.com
Date: Fri, Feb 15 2002 16:54:30 -0800
To: meetings@example.net
Message-Id: <12345.abc@newyork.example.com>
Subject: here’s a sample
```

Example 6: Headers reporting results from multiple MTAs in different domains

In this example we see multi-tiered authentication with an extended trust boundary.

The message was sent from someone at example.com’s New York office (newyork.example.com) to a mailing list managed at an intermediary. The message was signed at the origin using [DKIM].

The message was sent to a mailing list service provider called
example.net which is used by example.com. There meetings@example.net is expanded to a long list of recipients, one of which is at the Chicago office. In this example, we will assume that the trust boundary for chicago.example.com includes the mailing list server at example.net.

The mailing list server there first authenticated the message and affixed an Authentication-Results: header field indicating such. It then altered the message by affixing some footer text to the body including some administrivia such as unsubscription instructions. Finally, the mailing list server affixes a second [DKIM] signature and begins distribution of the message.

The border MTA for chicago.example.com explicitly trusts results from mail-router.example.net so that header is not removed. It performs evaluation of both signatures and determines that the first (most recent) is a "pass" but, because of the aforementioned modifications, the second is a "hardfail". However, the first signature included the Authentication-Results: header added at mail-router.example.net which validated the second signature. Thus, indirectly, it can be determined that the authentication claimed by both signatures are indeed valid.
Appendix D. Public Discussion

[REMOVE BEFORE PUBLICATION]

Public discussion of this proposed specification is handled via the mail-vet-discuss@mipassoc.org mailing list. The list is open. Access to subscription forms and to list archives can be found at http://mipassoc.org/mailman/listinfo/mail-vet-discuss.
Author’s Address

Murray S. Kucherawy
Sendmail, Inc.
6475 Christie Ave., Suite 350
Emeryville, CA 94608
US

Phone: +1 510 594 5400
Email: msk+ietf@sendmail.com