

Individual submission  
Internet-Draft  
Intended status: Standards Track  
Expires: October 19, 2009

M. Kucherawy  
Sendmail, Inc.  
April 17, 2009

IMAP Annotation for Indicating Message Authentication Status  
draft-kucherawy-sender-auth-imap-01

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

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 October 19, 2009.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (<http://trustee.ietf.org/license-info>). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Internet-Draft Authentication-Results IMAP Annotation

April 2009

## Abstract

This memo defines an application of the IMAP (Internet Message Access Protocol) Annotations facility whereby a server can store and retrieve meta-data about a message relating to message authentication tests performed on the message and the corresponding results.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">1.1.</a>	Purpose . . . . .	<a href="#">3</a>
<a href="#">1.2.</a>	Definitions . . . . .	<a href="#">4</a>
<a href="#">2.</a>	SMTP Server or MDA Implementation . . . . .	<a href="#">6</a>
<a href="#">3.</a>	IMAP Server Implementation . . . . .	<a href="#">7</a>
<a href="#">4.</a>	IMAP Client Implementation . . . . .	<a href="#">8</a>
<a href="#">5.</a>	IMAP Annotation Format . . . . .	<a href="#">9</a>
<a href="#">6.</a>	Conformance and Usage Requirements . . . . .	<a href="#">10</a>
<a href="#">7.</a>	IANA Considerations . . . . .	<a href="#">11</a>
<a href="#">7.1.</a>	Annotation Registration . . . . .	<a href="#">11</a>
<a href="#">8.</a>	Security Considerations . . . . .	<a href="#">12</a>
<a href="#">8.1.</a>	Misleading Results . . . . .	<a href="#">12</a>
<a href="#">8.2.</a>	Attacks Against Authentication Methods . . . . .	<a href="#">12</a>
<a href="#">8.3.</a>	Intentionally Malformed Data . . . . .	<a href="#">12</a>
<a href="#">8.4.</a>	Compromised Internal Hosts . . . . .	<a href="#">12</a>
<a href="#">9.</a>	References . . . . .	<a href="#">13</a>
<a href="#">9.1.</a>	Normative References . . . . .	<a href="#">13</a>
<a href="#">9.2.</a>	Informative References . . . . .	<a href="#">13</a>
<a href="#">Appendix A.</a>	Acknowledgements . . . . .	<a href="#">15</a>
<a href="#">Appendix B.</a>	Examples . . . . .	<a href="#">16</a>
<a href="#">Appendix C.</a>	Public Discussion . . . . .	<a href="#">17</a>
	Author's Address . . . . .	<a href="#">18</a>

Internet-Draft Authentication-Results IMAP Annotation

April 2009

## 1. Introduction

Electronic mail, though ubiquitous and highly useful, is also prone to increasing abuse by parties that choose to exploit its lenient design for nefarious purposes such as "spam" and "phishing." Abuse of this leniency has become so widespread as to become an economic problem. Several nascent methods of mitigating this problem such as [\[SPF\]](#) and [\[DKIM\]](#) appear to make strides in this direction but are themselves not sufficient. In many cases the results of attempts to authenticate messages must be relayed to the user for final disposition.

This memo defines a new annotation for [\[IMAP\]](#) using the IANA Considerations found in [\[ANNOTATE\]](#) which is used to store and relay message authentication results from upstream (e.g. "border") mail servers to internal mail servers which ultimately do message delivery. This information can then be used by delivery agents or even the users themselves when determining whether or not the content of such messages is trustworthy.

The message header defined in [\[AUTH-RESULTS\]](#) serves a similar purpose and is simple to implement but has some moderate security implications, so a more secure channel is required. In particular, the header block of a message is generally unauthenticated and is also typically relayed intact, meaning it is an obvious vector for data forgery. Thus, trusting part of a message header to be secure is a difficult problem. This method and that of [\[I-D.DRAFT-KUCHERAWY-SENDER-AUTH-ESMTP\]](#) establishes a much better trust boundary and removes that obvious attack vector.

[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 electroic mail servers.

## 1.1. Purpose

The IMAP annotation 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;

Kucherawy

Expires October 19, 2009

[Page 3]

---

Internet-Draft Authentication-Results IMAP Annotation

April 2009

3. Create an extensible framework for specifying results from 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;
5. Do all of this in a way not prone to forgery or misinterpretation.

## 1.2. 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](#).

An "MTA" is a Mail Transfer Agent, or any agent which uses [[SMTP](#)] or its extensions to format and transport a message.

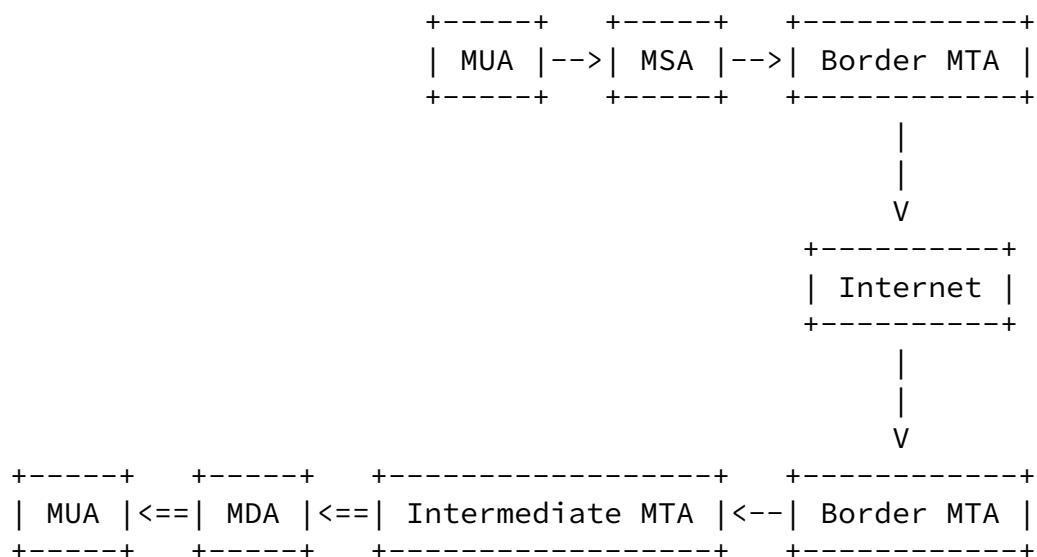
An "MDA" is a Mail Delivery Agent (also sometimes referred to as "LDA" or Local Delivery Agent), or any agent which has access to receive a message from an MTA and write it into the receiving user's "inbox".

An "MUA" is a Mail User Agent, or any software which retrieves and displays messages on behalf of a user.

A "border MTA" is an MTA which acts as a gateway between the general

Internet and the users within an organizational boundary.

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.

In the figure shown above, the double-lines indicate the portions of the transport of a message where this protocol would be applied. Note also that the Local Mail Transfer Protocol [[LMTP](#)] could benefit from a similar extension.

## [2.](#) SMTP Server or MDA Implementation

Within the message flow depicted in [Section 1.2](#), message authentication methods can be applied in a variety of places, most commonly the Border MTA, an Intermediate MTA, or the MDA.

Where the MDA does the message authentication, its results can be attached, using the annotation defined defined by this memo, to the message for later retrieval by an [[IMAP](#)] client. Where the message authentication takes place at one of the earlier MTAs, some method of carrying those results along each hop until mailbox injection at the MDA must be applied. One such proposal can be found in [[I-D.DRAFT-KUCHERAWY-SENDER-AUTH-ESMTP](#)] and another in [[AUTH-RESULTS](#)], but no specific method is required by this memo.

If [[AUTH-RESULTS](#)] is used, the header field MAY be deleted on delivery as the data relayed there will be reported via the annotation defined by this memo.

An MDA MAY choose to file messages other than in a recipient's message inbox, or discard it altogether, when certain criteria, such as failed authentications, are met.

### [3.](#) IMAP Server Implementation

An [[IMAP](#)] server conforming to this specification MUST implement [[ANNOTATE](#)] and MUST report these annotations to the client if they are attached to the message(s) being requested.

The name and format of the annotation can be found in [Section 5](#) and [Section 7](#).

The [\[IMAP\]](#) server itself may do the message authentication prior to serving the message to the client, or the MDA or one of the upstream MTAs may do so. In the former case, the authentication is being done after delivery and the results could be different (e.g. signatures could expire, sender policies could change, etc.). It is important to be aware that the results of authentication methods evaluated by this server could be notably different from those results returned during the original transit of the message. At the time this memo was prepared, all known methods were intended for evaluation at time of delivery, not at the time the message is served to the end user.



An [\[IMAP\]](#) client conforming to this specification will request the "authresults" annotation when retrieving a message, and render those results to users in some meaningful way.

The name and format of the annotation can be found in [Section 5](#) and [Section 7](#).

## 5. IMAP Annotation Format

The content of the annotation, as defined using [\[ABNF\]](#), MUST be formatted as follows:

```
authres = version ":" authserv-id ":" 1*resinfo
          ; relays a single unit of authentication results
          ; information
```

The "version", "authserv-id" and "resinfo" are as defined in [Section 2.2](#) of [\[AUTH-RESULTS\]](#). The "version" refers to the version of this memo, not the version of [\[AUTH-RESULTS\]](#) referenced here.

## 6. Conformance and Usage Requirements

[Section 2](#), [Section 3](#) and [Section 4](#) specify the only requirements for conformance to this specification.

---

Internet-Draft Authentication-Results IMAP Annotation

April 2009

## [7.](#) IANA Considerations

### [7.1.](#) Annotation Registration

Per [[IANA-CONSIDERATIONS](#)], IANA is requested to register this new IMAP annotation as per [[ANNOTATE](#)]. The template to be registered is as follows:

To: iana@iana.org  
Subject: IMAP Annotate Registration

Please register the following IMAP Annotate item:

[X] Entry            [ ] Attribute

Name:    /authresults

Description: Results of message authentication tests, as  
              specified in [[AUTH-RESULTS](#)]

Content-Type: text-plain; charset=us-ascii

Contact person: Murray S. Kucherawy

Contact email: msk@sendmail.com

## [8.](#) Security Considerations

The following security considerations apply when applying or processing the authresults IMAP annotation:

### [8.1.](#) Misleading Results

Until some form of service for querying the reputation of a sending agent is widely deployed, the existence of this annotation 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, which might be a spammer or a compromised system).

### [8.2.](#) Attacks Against Authentication Methods

If an attack becomes known against an authentication method, clearly then the agent verifying that method can be fooled into thinking an inauthentic message is authentic, and thus the value of this annotation can be misleading. It follows that any attack against the authentication methods supported by this document (and later amendments to it) is also a security consideration here.

### [8.3.](#) Intentionally Malformed Data

It is possible for an attacker to include data in a message which is extraordinarily large or otherwise malformed in an attempt to discover or exploit weaknesses in parsing code. Implementors must thoroughly verify all such data received from [\[IMAP\]](#) servers and be robust against intentionally as well as unintentionally malformed data.

#### [8.4.](#) Compromised Internal Hosts

An internal MUA or MTA which has been compromised could generate mail with forged data, eventually generating an annotation which endorses it. Although it is clearly a larger concern to have compromised internal machines than it is to prove the value of this proposal, this risk can be mitigated by arranging that internal MDAs not attach this data if it claims to have been added by a trusted border MTA (as described above) yet the [\[SMTP\]](#) connection is not coming from an internal machine known to be running an authorized MTA. However, in such a configuration, legitimate MDAs will have to add this data when legitimate internal-only messages are generated.

## [9.](#) References

### [9.1.](#) Normative References

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

[ANNOTATE] Daboo, C. and R. Gellens, "IMAP ANNOTATE Extension", [RFC 5257](#), June 2008.

[AUTH-RESULTS] Kucherawy, M., "Message Header Field for Indicating Message Authentication Status", [RFC 5451](#), April 2009.

[IMAP] Crispin, M., "Internet Message Access Protocol - Version 4rev1", [RFC 3501](#), March 2003.

## [9.2.](#) Informative References

- [AUTH] Myers, J., "SMTP Service Extension for Authentication", [RFC 2554](#), March 1999.
- [DKIM] Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, "DomainKeys Identified Mail (DKIM) Signatures", [RFC 4817](#), May 2007.
- [DOMAINKEYS] Delany, M., "Domain-based Email Authentication Using Public Keys Advertised in the DNS (DomainKeys)", [RFC 4870](#), May 2007.
- [I-D.DRAFT-CROCKER-EMAIL-ARCH] Crocker, D., "Internet Mail Architecture", I-D [draft-crocker-email-arch](#), May 2007.
- [I-D.DRAFT-KUCHERAWY-SENDER-AUTH-ESMTP] Kucherawy, M., "SMTP Service Extension for Indicating Message Authentication Status", I-D [draft-kucherawy-sender-auth-esmtp-01](#), September 2008.
- [IANA-CONSIDERATIONS] Alvestrand, H. and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", [RFC 2434](#), October 1998.
- [LMTP] Meyers, J., "Local Mail Transport Protocol", [RFC 2033](#), October 1996.

Kucherawy

Expires October 19, 2009

[Page 13]

---

Internet-Draft Authentication-Results IMAP Annotation

April 2009

- [SENDERID] Lyon, J. and M. Wong, "Sender ID: Authenticating E-Mail", [RFC 4406](#), April 2006.
- [SMTP] Klensin, J., "Simple Mail Transfer Protocol", [RFC 2821](#), April 2001.
- [SPF] Wong, M. and W. Schlitt, "Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1", [RFC 4408](#), April 2006.

#### [Appendix A](#). Acknowledgements

The author wishes to acknowledge the following for their review and constructive criticism of this proposal: (add names here)





## [Appendix B](#). Examples

This section presents some examples of the use of this IMAP annotation.

(add examples here)

---

Internet-Draft Authentication-Results IMAP Annotation

April 2009

[Appendix C](#). 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>.

Internet-Draft    Authentication-Results IMAP Annotation

April 2009

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](mailto:msk+ietf@sendmail.com)

Kucherawy

Expires October 19, 2009

[Page 18]