

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

M. Kucherawy
Sendmail, Inc.
April 17, 2009

Indicating Message Authentication System Parameters
draft-kucherawy-sender-auth-caps-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 Message Authentication System Parameters

April 2009

Abstract

This memo defines simple extensions to IMAP, POP3 and SMTP to permit a user's message reading software (Mail User Agent, or MUA) to determine the properties of its environment with respect to available message authentication services.

Table of Contents

1.	Introduction	3
2.	Definitions	4
3.	SMTP AUTHSERV Extension	6
3.1.	Description	6
3.2.	Framework for the AUTHSERV SMTP Extension	6
3.3.	Details	6
4.	IMAP AUTHSERV Capability	8
5.	POP3 AUTHSERV Capability	9
6.	Using DNS to Advertise Authentication Service	10
7.	Conformance and Usage Requirements	11
8.	IANA Considerations	12
8.1.	SMTP Extension Registration	12
8.2.	IMAP Extension Registration	12
8.3.	POP3 Extension Registration	12
9.	Security Considerations	13
10.	References	14
10.1.	Normative References	14
10.2.	Informative References	14
Appendix A.	Acknowledgements	15
Appendix B.	Examples	16
B.1.	Example use of SMTP extension	16
B.2.	Example use of IMAP extension	17
B.3.	Example use of POP3 extension	18
Appendix C.	Public Discussion	19
	Author's Address	20

Internet-Draft Message Authentication System Parameters

April 2009

1. Introduction

The message header field defined in [[AUTH-RESULTS](#)] can be used to relay to MUAs or other internal filtering agents the results of message authentication efforts performed by upstream Mail Transport Agents (MTAs). As messaging is generally not secure by default, there exist some vectors for allowing forgeries of that header field through to user agents or filters which might then take inappropriate action. (See the Security Considerations section of that memo for details.)

Part of the work required to secure those vectors involves securing the channel between MTAs and user agents such that the contents of the header field can be trusted. Another important need is to handle the configuration of that channel as automatically as possible.

There are two important facilities needed toward this end:

1. An [[SMTP](#)] extension: User agents can contact upstream MTAs within their administrative domains to see if those MTAs are conforming to the security requirements of [[AUTH-RESULTS](#)], and possibly also determine what token(s) those MTAs use when generating Authentication-Results header fields.
2. [[IMAP](#)] and/or [[POP3](#)] extensions: User agents can contact their message store servers to determine what token(s) authorized MTAs use when generating the authentication results header fields, which also implicitly notifies the MUA that the administrative domain conforms to the security requirements of [[AUTH-RESULTS](#)].

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](#).

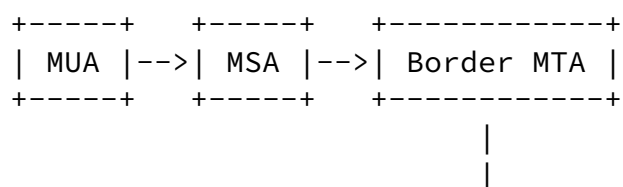
An "MTA" is a Mail Transfer Agent, or any agent which uses [[SMTP](#)] or its extensions to format and transport a message.

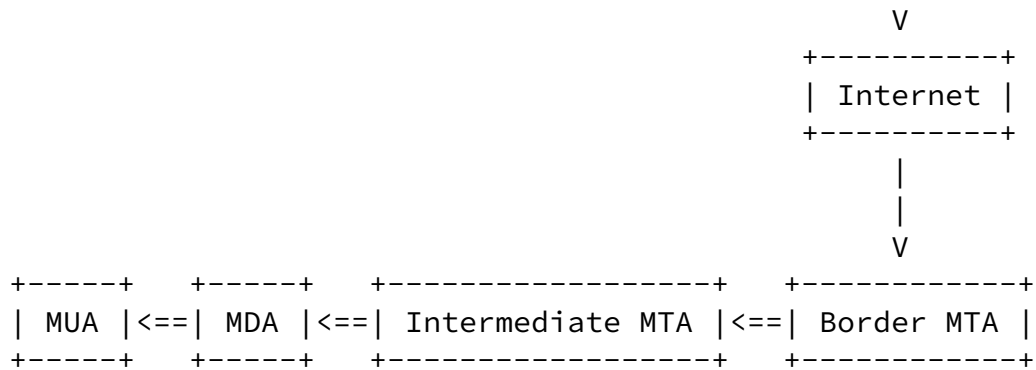
An "MDA" is a Mail Delivery Agent (also sometimes referred to as "LDA" or Local Delivery Agent), or any agent which has access to receive a message from an MTA and write it into the receiving user's "inbox".

An "MUA" is a Mail User Agent, or any software which retrieves and displays messages on behalf of a user. It may use [[IMAP](#)] or [[POP3](#)].

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.

"authserv-id" is imported from [[AUTH-RESULTS](#)].

[3.](#) SMTP AUTHSERV Extension

[3.1.](#) Description

This section defines a new [[SMTP](#)] extension which enables user agents and downstream filters to interrogate an MTA as to whether or not it conforms to the security requirements of [[AUTH-RESULTS](#)]. In particular, it reveals (a) that it conforms to that memo's requirements, and (b) what "authserv-id" that MTA uses when adding Authentication-Results header fields to messages inbound.

[3.2.](#) Framework for the AUTHSERV SMTP Extension

Per the requirements of [[SMTP](#)], the framework for the AUTHSERV Extension is as follows:

1. The name of the SMTP service extension is "Authserv-ID";
2. The SMTP buffer length is extended by 256 bytes on servers offering this service extension;
3. The EHLO keyword value associated with the extension is AUTHSERV;
4. The parameter used with the AUTHRES EHLO keyword is an "authserv-id" as defined above, and is optional;
5. No additional parameters are added to the MAIL command;
6. No additional parameters are added to the RCPT command;
7. No additional SMTP verbs are defined by this extension; and
8. The next subsection discusses how support for the extension affects the behaviour of a server and client SMTP session.

[3.3.](#) Details

If an MTA is compliant with that specification, it SHOULD use this extension to advertise the "authserv-id" it uses when generating new Authentication-Results header fields. An MUA can then use SMTP to query the upstream MTA by issuing an EHLO command to determine whether or not the MTA implements the specification in the header field memo and also what "authserv-id" it should expect. Once the presence or absence of this information is determined by the MUA, it would simply issue a QUIT command and disconnect.

The SMTP server MAY choose not to include the "authserv-id" token in use if there is some practical reason to do so. In this case, the

server is simply announcing that it conforms to the remaining security issues discussed in [[AUTH-RESULTS](#)].

This SMTP extension adds no new SMTP functionality per se. Rather, it simply provides a means for an MUA attempting to implement [[AUTH-RESULTS](#)] to acquire important security information about its environment.

A new [[IMAP](#)] capability called AUTHSERV is defined.

Prior to authentication, it has no value associated with it, i.e. the capability reported is simply "AUTHSERV". After authentication, it always has a value associated with it, namely the "authserv-id" string used within the administrative domain represented by the IMAP server to declare validated authentication results, i.e. it becomes "AUTHSERV=authserv-id".

The [[ABNF](#)] defining the capability's syntax is as follows:

```
authserv-cap := AUTHSERV [ "=" authserv-id ]
```

The advertisement of this capability to a client

1. MAY be considered by the client to be a statement that the administrative domain is compliant with the security requirements of [[AUTH-RESULTS](#)]; and
2. in the post-authentication form, contains the "authserv-id" string which will be present on all Authentication-Results header fields which the client can use when determining courses of action based on the results of prior message authentication efforts.

5. POP3 AUTHSERV Capability

The formal definition, per [[POP3-CAPA](#)]:

CAPA tag: AUTHSERV

Arguments: "authserv-id" string used within the administrative domain

Added commands: none

Standard commands affected: none

Announced states / possible differences: both / yes (see below)

Commands valid in states: n/a

Specification reference: this document

Discussion: A new [[POP3](#)] capability called AUTHSERV is defined. It MUST have a value associated with it in the TRANSACTION state, namely the "authserv-id" string used within the administrative domain represented by the POP3 server to declared validated authentication results. It MUST NOT have a value in the AUTHENTICATION state. The advertisement of this capability to a client

1. MAY be considered by the client to be a statement that the administrative domain is compliant with the security requirements of [[AUTH-RESULTS](#)]; and
2. contains the "authserv-id" string which will be present on all Authentication-Results header fields which the client could use when determining courses of action based on the results of prior message authentication efforts.

[6.](#) Using DNS to Advertise Authentication Service

An ADMD can place the "authserv-id" token in a text resource record (TXT) for MUAs to query. For this purpose, the label "_authservid" is reserved in the DNS namespace at the same location as the top of the ADMD.

The name for the label "_authservid" was chosen because any domain name that includes it as one of its labels cannot be a valid host name. There will never be any accidental overlap with a valid domain name. Further, it is safe to create a rule that says that a TXT DNS record that comes from a domain name that includes a "_authservid" label will always have the content defined in this document.

7. Conformance and Usage Requirements

[Section 3](#), [Section 4](#) and [Section 5](#) are each individual specifications containing proposals supporting the goals specified in [Section 1](#) and in [\[AUTH-RESULTS\]](#). Use of them in any combination (other than "none") constitutes minimal conformance to this specification and support of the header field memo.

[8.](#) IANA Considerations

This section discusses actions requested by IANA, per [\[IANA-CONSIDERATIONS\]](#).

[8.1.](#) SMTP Extension Registration

IANA is requested to register the AUTHSERV extension to SMTP, referencing this memo as its defining document.

[8.2.](#) IMAP Extension Registration

This document constitutes registration of the AUTHSERV IMAP capability in the imap4-capabilities registry.

[8.3.](#) POP3 Extension Registration

This document constitutes registration of the AUTHSERV POP3 capability in the pop3-extension-mechanism registry.

9. Security Considerations

This memo serves to address some of the security considerations within [[AUTH-RESULTS](#)]. In particular, the focus of this memo is to provide the means to determine automatically whether the administrative domain in which an MUA finds itself is (or claims to be) conformant with the security considerations of that memo, and furthermore to acquire a key piece of information to be used in carrying out the work described there. It is not an attempt to resolve any of those considerations, other than simplifying to some extent the work of configuring MUAs, thus leaving fewer places for misconfigurations to occur and security problems to form.

Consult that document for further discussion of security issues.

[10.](#) References

[10.1.](#) Normative References

- [ABNF] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", [RFC 5234](#), January 2008.
- [IMAP] Crispin, M., "Internet Message Access Protocol - Version 4rev1", [RFC 3501](#), March 2003.
- [POP3-CAPA]

Gellens, R., Newman, C., and L. Lundblade, "POP3 Extension Mechanism", [RFC 2449](#), November 1998.

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

[10.2.](#) Informative References

[AUTH-RESULTS]

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

[I-D.DRAFT-CROCKER-EMAIL-ARCH]

Crocker, D., "Internet Mail Architecture", [draft-crocker-email-arch](#) (work in progress), May 2007.

[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.

[POP3] Meyers, J. and M. Rose, "Post Office Protocol - Version 3", [RFC 1939](#), May 1996.

[Appendix A.](#) Acknowledgements

The author wishes to acknowledge the following for their review and constructive criticism of this proposal: Alexey Melnikov

[Appendix B](#). Examples

This section presents some examples of the use of these extensions. In all cases, "C:" represents a transmission by the client and "S:" represents a transmission by the server.

[B.1](#). Example use of SMTP extension

An example use of the AUTHSERV SMTP extension:

```
C: (establishes connection to SMTP server)
S: 220 server.example.com ESMTP; Fri, 10 Oct 2008 13:52:37 -0700 (PDT)
C: EHLO myname.example.com
S: 250-ENHANCEDSTATUSCODES
S: 250-PIPELINING
S: 250-8BITMIME
S: 250-SIZE
S: 250-DSN
S: 250-DELIVERBY
S: 250-AUTHSERV authserver.example.com
S: 250 HELP
C: QUIT
S: 221 server.example.com closing connection
S: (closes connection channel)
```

The client has connected to the SMTP server and issued the EHLO command to determine whether or not the SMTP server claims to support the requirements of the header memo. From this the client learns that in fact it does conform, and furthermore knows what "authserv-id" will be used by this MTA when communicating authentication results.

[B.2.](#) Example use of IMAP extension

An example use of the AUTHSERV IMAP capability (server replies wrapped here for legibility):

```
C: (establishes connection to IMAP server)
S: * OK IMAP server IMAP4rev1 ready
C: x CAPABILITY
S: * CAPABILITY CAPABILITY IMAP4 IMAP4rev1 UIDPLUS
    AUTHSERV
S: x OK CAPABILITY COMPLETED
    (authentication takes place)
C: x CAPABILITY
S: * CAPABILITY CAPABILITY IMAP4 IMAP4rev1 UIDPLUS
    AUTHSERV=authserv.example.com
S: x OK CAPABILITY COMPLETED
    (session continues)
```

The client connects and requests capabilities, immediately learning that this administrative domain complies with the security requirements of the header memo. After authentication, the client issues a second request for capabilities at which point the local "authserv-id" in use is revealed.

[B.3.](#) Example use of POP3 extension

An example use of the AUTHSERV POP3 capability (server replies wrapped here for legibility):

```
C: (establishes connection to IMAP server)
S: +OK POP3 server ready
C: CAPA
S: +OK Capability list follows
S: TOP
S: USER
S: SASL CRAM-MD5
S: RESP-CODES
S: AUTHSERV
S: .
(authentication takes place)
C: CAPA
S: +OK Capability list follows
S: TOP
S: USER
S: SASL CRAM-MD5
S: RESP-CODES
S: AUTHSERV authserv.example.com
S: .
(session continues)
```

The client connects and requests capabilities, immediately learning that this administrative domain complies with the security requirements of the header memo. After authentication, the client issues a second request for capabilities at which point the local "authserv-id" in use is revealed.

[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>.

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

