

Individual submission
Internet-Draft
Updates: [5451](#), [6376](#) (if approved)
Intended status: Standards Track
Expires: August 23, 2012

M. Chew
Google, Inc.
M. Kucherawy
Cloudmark, Inc.
February 20, 2012

Original-Authentication-Results Header Field
draft-kucherawy-original-authres-00

Abstract

This memo defines a message header field for relaying message authentication results. The new field differs from the existing Authentication-Results message header field in that it is specifically used to relay message authentication results from one administrative domain to another.

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 August 23, 2012.

Copyright Notice

Copyright (c) 2012 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 (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as

Internet-Draft

Original-Auth-Results Header Field

February 2012

described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
2.	Definitions	3
2.1.	Keywords	3
2.2.	Email Architecture	3
3.	Handling Sequence	4
4.	Definition	4
5.	Adding the Header Field	5
6.	Processing the Header Field	5
7.	DKIM Functional Extension	5
8.	IANA Considerations	6
9.	Security Considerations	6
9.1.	Trust Is Subjective	6
10.	References	6
10.1.	Normative References	6
10.2.	Informative References	6
Appendix A.	Original-Authentication-Results Examples	7
A.1.	Relayed Authentication Results	8
A.2.	Relaying Original Results	9
Appendix B.	Acknowledgements	9

Internet-Draft

Original-Auth-Results Header Field

February 2012

1. Introduction

[AUTHRES] defines a new header field for email that presents the results of a message authentication effort in a machine-readable format. It thus introduced a mechanism for relaying message-level authentication results from a mail server running on a border system to internal hosts. This created a trusted channel between border mail servers and internal agents relaying the results of that authentication work. That document also created rules for ensuring those data can be trusted by specifying under what circumstances instances of that field should be removed prior to delivery.

Some sites wish to take into consideration such authentication results claimed by trusted intermediaries, effectively extending the trusted channel to specific external entities. Although [AUTHRES] includes support for this notion, this separate mechanism is simpler, more robust, and requires no changes to existing authentication infrastructure.

Therefore, this document defines a new field called Original-Authentication-Results. The content of the field is identical to that specified in [AUTHRES]. This field is required to be unique, appearing only once in a message, and thus it is possible to determine conclusively whether or not it is included in the part of the header covered by a signature. The presence of multiple instances of this field in a message would be an indication of either an implementation error or the injection of a fraudulent claim. This "single instance" constraint enables the relaying of the results of message authentication work as it was received for the first time by a participating MTA.

The relationship between [AUTHRES] and this header field is analogous to the relationship between [SMTP] and [MSA].

2. Definitions

[2.1.](#) Keywords

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](#)].

[2.2.](#) Email Architecture

Readers are encouraged to be familiar with the material found in [[EMAIL-ARCH](#)]. Some terms used in this memo are defined there.

[3.](#) Handling Sequence

This section describes the intended use of the field by all parties being considered.

Suppose a user A sends an email to mailing list B. The message is signed with [[DKIM](#)]. Upon arrival at B, the MTA evaluates A's DKIM signature, producing a result. The mailing list at B alters the message in some way that causes the DKIM signature become invalid. B then relays the message to all of the mailing list's current subscribers, which includes C. Upon arrival at C, the message again has its DKIM signatures evaluated, but this time it fails. Any privileged treatment at C that would normally be afforded a message signed by A is lost because of the mailing list software's alterations of the original.

If, however, C could declare that it trusts that B's email infrastructure properly implements DKIM and is also otherwise generally secure, then any statements by B about A's signature could be trusted. This means C could once again give A's mail preferential treatment as long as it arrived at B with a still-valid DKIM signature.

The header field introduced here provides a mechanism to make such a statement, and provides the rules under which the claims made by B can be believed and applied.

[4.](#) Definition

This memo adds a new header field to the "Permanent Message Header Field Registry", as follows:

Header field name: Original-Authentication-Results

Applicable protocol: mail

Status: standard

Author/Change controller: IETF

Specification document(s): [this memo]

Related information: [[AUTHRES](#)]

[5.](#) Adding the Header Field

A processing agent adding this field SHOULD NOT add this field if one already exists, as presumably any earlier handling agents were closer to the origination of the message. If it does, it MUST remove all existing instances of this field before adding a new one.

The syntax of this field MUST conform to [[AUTHRES](#)] and its extensions.

This header field SHOULD be prepended to the existing header rather than being added any other place in the header so that some idea of where or when it was added can be determined. It SHOULD be handled as trace information as defined in [[SMTP](#)].

The added field MUST be included in the portion of the header of the message covered by a signature added by that agent's ADMD, using [[DKIM](#)] or another mechanism of equivalent or stronger security semantics. The "d=" of the added signature MUST match the authserv-id (see Section 2.3 of [[AUTHRES](#)]) included in the header field being added.

6. Processing the Header Field

An agent receiving a message with more than one instance of this field MUST ignore all of them. The field MUST also be ignored if it is not covered by a signature added by the trusted third party named in the authserv-id portion of the field.

The choice of which external parties' authentication results are to be trusted is entirely an operational one and not specified here. Presumably this is enabled explicitly and only by prior arrangement after appropriate dialogue and system auditing has been done. If this field is observed on a message and appears not to have been added by a trusted agent, it MUST be ignored.

An instance of this header field that satisfies these restrictions SHOULD be treated as semantically equivalent to an [\[AUTHRES\]](#) field added by the evaluating ADMD.

7. DKIM Functional Extension

The function defined by [\[DKIM\]](#) accepts a message as input and includes the following as its outputs:

1. A result as to the outcome of the validation attempt of each signature (e.g. pass or fail, possibly with a more descriptive error code);

2. The name of the domain that attached each signature, namely the value of the "d=" tag in each signature;
3. Optionally, the name of the signing identity found in the signature, namely the value of the "i=" tag in each signature.

To satisfy the signature requirement specified in [Section 4](#), a DKIM API would need to be extended to include an indication of whether or not the header field defined by this memo was covered by a signature.

8. IANA Considerations

IANA is requested to add this new field, as defined in [Section 4](#), to the Email Permanent Header Field Registry.

[9.](#) Security Considerations

This section discusses security issues regarding the handling of this new header field.

[9.1.](#) Trust Is Subjective

A malicious sender could generate a message compliant with this specification, asserting that the original message authenticates from some valued domain. Recipients will need to be sure to separately vet the list of domains they trust, and perhaps do periodic audits of both the list and the other ADMDs on it.

[10.](#) References

[10.1.](#) Normative References

- [AUTHRES] Kucherawy, M., "Message Header Field for Indicating Message Authentication Status", [RFC 5451](#), April 2009.
- [KEYWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

[10.2.](#) Informative References

- [DKIM] Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, "DomainKeys Identified Mail (DKIM) Signatures", [RFC 4871](#), May 2007.
- [EMAIL-ARCH] Crocker, D., "Internet Mail Architecture", [RFC 5598](#), July 2009.
- [MSA] Gellens, R. and J. Klensin, "Message Submission",

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

[Appendix A.](#) Original-Authentication-Results Examples

This section presents an example of the use of this new header field

to indicate trustable message authentication results added by an intermediary.

A message that contains basic relayed authentication information:

```
Authentication-Results: border.example.org;
    dkim=pass header.d=example.net;
    dkim=fail header.d=example.com
DKIM-Signature: a=rsa-sha256; c=relaxed/simple; s=test;
    d=example.net;
    h=From:Date:To:Subject:Message-Id:Authentication-Results;
    bh=8hsafun...9813=;
    b=xkBnyZc0z...dscC5j9eAw0q2yFz43aYD8==
Authentication-Results: lists.example.net; dkim=pass
    header.d=example.com
Received: from mail-router.example.com
    (mail-router.example.com [192.0.2.250])
    by lists.example.net (8.11.6/8.11.6)
    with ESMTP id g11Lkr60042377;
    Fri, Feb 15 2002 17:19:22 -0800
DKIM-Signature: a=rsa-sha256; c=relaxed/simple; s=test;
    d=example.com; h=From:Date:To:Subject:Message-Id;
    bh=sa98djf...ffdf=;
    b=BvC+mpYILJo...u1n6RUcGxJs0LULya8Kg==
Received: from internal-0-2-1.example.com
    (internal-0-2-1.example.com [192.0.2.1])
    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.com
Date: Fri, Feb 15 2002 16:54:30 -0800
To: sample-list@example.net
Message-Id: <12345.abc@example.com>
Subject: [sample] here's a sample
```

Hello! Goodbye!

An example showing a message that transited a list and shows the authentication work done enroute

This is an example of a message that went from an author domain (example.com) via a mailing list called sample@example.net, which then relayed the message to receiver@example.org, who is subscribed to that list.

The original message was validated by the list server, as reflected in an Authentication-Results field added by the list software.

Since the list software is configured to add a tag prefix to the

Subject: field, the DKIM signature from example.com is invalidated. However, the Authentication-Results added at example.net is asserting that the original signature was valid when it was received. To assert the validity of that claim, the new Authentication-Results field is signed as well.

Finally, example.org, which explicitly trusts example.net in this illustration, can believe that the original message contained a valid signature from example.com.

[now explain what problem isn't covered here]

[A.2.](#) Relaying Original Results

A message that contains relayed authentication information that can be trusted:

(example message)

[describe what's going on in the example]

[now explain how this solves the problem]

[Appendix B.](#) Acknowledgements

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

Authors' Addresses

Monica Chew
Google, Inc.
345 Spear St.
San Francisco, CA 94105
US

Phone: +1 650 253 0000
EMail: mmc@google.com

Internet-Draft

Original-Auth-Results Header Field

February 2012

Murray S. Kucherawy
Cloudmark, Inc.
128 King St., 2nd Floor
San Francisco, CA 94107
US

Phone: +1 415 946 3800
EMail: msk@cloudmark.com

