

Network Working Group
Internet-Draft
Intended status: Experimental
Expires: August 27, 2011

D. Crocker
Brandenburg InternetWorking
M. Kucherawy
Cloudmark
February 23, 2011

MIME Content Authentication using DOSETA (MIMEAUTH)
draft-crocker-doseta-mimeauth-00

Abstract

MIME is a method of packaging and labeling aggregations of data; it is used both for email and the Web. Many usage scenarios would benefit by having an objective method of assessing the validity of MIME data, based on an authenticated identity. MIMEAUTH leverages technology developed for DKIM to provide such a method. Its use can be extended to cover specific header-fields of a containing email message or World Wide Web HTTP content. Existing authentication mechanisms have achieved only limited success due to challenges with administration and use. MIMEAUTH has very low administration and use overhead, through self-certifying keys in the DNS and a labeling method that can be transparent to end-users. For relayed and mediated sequences, MIMEAUTH can be implemented within a service and therefore can be transparent to end-system software.

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 27, 2011.

Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

Internet-Draft

RFC4871bis

February 2011

This document is subject to [BCP 78](http://trustee.ietf.org/license-info) 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 described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
1.1.	Signing Identity	4
1.2.	Terminology and Definitions	4
1.3.	Open Issues	4
2.	Signing and Verifying Protocol	5
3.	Extensions to DOSETA Template	6
3.1.	Signature Data Structure	6
3.2.	Email Signed Header Fields	7
4.	Considerations	8
4.1.	Security Considerations	8
4.2.	IANA Considerations	9
5.	References	9
5.1.	Normative References	9
5.2.	Informative References	10
Appendix A.	Acknowledgements	10
	Authors' Addresses	10

Internet-Draft

RFC4871bis

February 2011

1. Introduction

MIME is a core data-packaging mechanism for Internet applications; it is used both for email and the Web. Many usage scenarios would benefit by having an objective method of assessing the validity of MIME data, based on an authenticated identity. Existing authentication mechanisms have achieved only limited use. MIMEAUTH is based on DOSETA [[I-D.DOSETA](#)] to provide such a method. Its use can be extended to cover specific header-fields of a containing email message or World Wide Web HTTP content. MIMEAUTH has very low administration and use overhead, through self-certifying keys in the DNS and a labeling method that can be transparent to end-users. For relayed and mediated sequences, MIMEAUTH can be implemented within a service and therefore can be transparent to end-system software.

The approach taken by MIMEAUTH differs from previous approaches to message authentication, such as Secure/Multipurpose Internet Mail Extensions (S/MIME) [[RFC1847](#)] and OpenPGP [[RFC4880](#)], in that:

- o the signature is written as an associated attribute in a header field, rather than being integrated into the data itself, so that neither human recipients nor existing MUA (Mail User Agent) software is confused by signature-related content appearing in the data;
- o there is no dependency on having public and private key pairs being issued by well-known, trusted certificate authorities;
- o there is no dependency on the deployment of any new Internet protocols or services for public key distribution or revocation;
- o authentication is distinct from encryption;

MIMEAUTH:

- o is compatible with the existing email and Web infrastructure and

- is transparent to it, to the fullest extent possible;
- o requires minimal new infrastructure;
- o can be implemented independently of clients in order to reduce deployment time;
- o can be deployed incrementally;
- o allows delegation of signing to third parties.

[1.1.](#) Signing Identity

MIMEAUTH separates specification of the identity of the MIMEAUTH signer from the purported author of the content. Verifiers can use the signing information to decide how they want to process the data. In particular, the authentication identity specified by a MIMEAUTH signature is not required to match any other identifier the content or the header. However when the identity does match other, specific identities, specific semantics are assigned.

[1.2.](#) Terminology and Definitions

This specification incorporates the terminology defined in [\[I-D.DOSETA\]](#).

Syntax descriptions use Augmented BNF (ABNF) [\[RFC5234\]](#).

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 [\[RFC2119\]](#).

Additional terminology:

Internal IDentifier (IID): An optional textual literal token that can be included with a signature and can be part of communications back to the signer, as a reference to the signature. For DOSETA processing, the domain name portion of

the IID has only basic domain name semantics; any possible owner-specific semantics are outside the scope of DOSETA. That is, for MIMEAUTH, the entire string is an undifferentiated literal. It is specified in [Section 3.1](#) .

[1.3](#). Open Issues

Still to be resolved:

- o Precise semantics of a signature. Does it merely declare "responsibility" by the signer, or "validity" of the content, or something else?
- o Should there be a flag that differentiates among different possible semantics, such as defaulting to "responsibility" but able to flag assertion of validity? How dangerous would such a flag be?

NOTE: A variety of assurances can be made about an email From: field, such as validity of the domain portion, validity of the entire email address, and validity of the <display-name> string. This, of course, is separate from whether to trust /any/ assurances being made...

[2](#). Signing and Verifying Protocol

MIMEAUTH uses the DOSETA "Generic Header/Content Signing Service Template" [[I-D.DOSETA](#)] as its base.

The DOSETA Template specifies features labeled TEMPLATE that need to be tailored to a specific signing service. For MIMEAUTH, the tailored features are:

Signature Association: The DOSETA-Signature data are stored in a MIME Content-Authentication: header field that is part of the MIME object being authenticated. This contains all of the signature and key-fetching data, per [[I-D.DOSETA](#)].

Semantics Signaling: The presence of a MIME Content-Authentication: header field signals the use of MIMEAUTH.

Semantics: A MIMEAUTH signature means that the owner of the DDI is taking direct responsibility for the signed content and for the content of any referenced header fields, if present. Hence, the payload, or output, of MIMEAUTH is:

- + The DDI domain name, specifically the "d" parameter in the MIME Content-Authentication: header field
- + A list of referenced header fields
- + An indication that the signature verified

NOTE: The semantics of this signature are much stronger than the semantics of a DKIM signature and pertain to the content, not merely the signing domain. [[RFC4871](#)]

Header/Content Mapping: MIMEAUTH maps the DOSETA header processing to the cited header fields that are associated with the MIME object. DOSETA Content maps to the MIME body, per [[RFC2045](#)]. The Content-type: header field is always covered by the signature.

When a MIMEAUTH signature lists additional header fields in the "h" parameter, MIMEAUTH is asserting that these also have valid data. By including other common header fields that are associated with MIME usage, the scope of a MIMEAUTH signature can apply to a containing protocol data unit, such as an email message or a Web payload. Therefore, when the authentication semantic is intended to assert validity of both the MIME data and the context in which it occurs, a minimum set of additional header fields SHOULD be included in the DOSETA "h" parameter. This is discussed further in [Section 3.2](#).

[3.](#) Extensions to DOSETA Template

This section contains specifications that are added to the basic

[3.1.](#) Signature Data Structure

These are MIMEAUTH-specific tags:

i= This specifies an Internal Identifier (IID) token that can be used when referring to the signed data, back to the signer. Within the MIMEAUTH protocol, the string has no value except as a literal token. Any conventions for the string that are imposed by the signer are unknown to other MIMEAUTH participants.

The syntax is the form of a standard email address where the <local-part> MAY be omitted.

Internationalized domain names MUST be converted using the steps listed in [Section 4 of \[RFC5890\]](#) using the "ToASCII" function.

ABNF:
sig-i-tag = %x69 [FWS] "=" [FWS]
 [local-part] "@" domain-name

z= Copied header fields (DOSETA-quoted-printable, but see description; OPTIONAL, default is null). A vertical-bar-separated list of selected header fields present when the message was signed, including both the field name and value. It is not required to include all header fields present at the time of signing. This field need not contain the same header fields listed in the "h=" tag. The header field text itself MUST encode the vertical bar ("|", %x7C) character. That is,

vertical bars in the "z=" text are meta-characters, and any actual vertical bar characters in a copied header field MUST be encoded. Note that all whitespace MUST be encoded, including whitespace between the colon and the header field value. After encoding, FWS MAY be added at arbitrary locations in order to avoid excessively long lines; such whitespace is NOT part of the value of the header field, and MUST be removed before decoding.

Copied header field values are for diagnostic use.

Header fields with characters requiring conversion SHOULD be converted as described in MIME Part Three [[RFC2047](#)].

ABNF:

```
sig-z-tag      = %x7A [FWS] "=" [FWS]
                  sig-z-tag-copy
                  *( "|" [FWS] sig-z-tag-copy )
sig-z-tag-copy = hdr-name [FWS] ":"
                  qp-hdr-value
```

[3.2.](#) Email Signed Header Fields

Some header fields have semantics that are relevant to end users and often are presented to them. If MIMEAUTH is used to sign an email message, it is useful to cover such header fields, in addition to the MIME content. This section provides a generic recommendation intended to apply to the general case of signing a message; specific senders might wish to modify these guidelines as required by their unique situations. Verifiers MUST be capable of verifying signatures even if one or more of the recommended header fields is not signed or if one or more of the dis-recommended header fields is signed. Note that verifiers do have the option of ignoring signatures that do not cover a sufficient portion of the header or content, just as they might ignore signatures from an identity they do not trust.

The signer is encouraged to consider carefully which fields are

important to the interpretation of the content and which ones are not. As an example, note what fields are typically displayed to recipients. The following header fields are listed as a default set and SHOULD be included in the signature, if they are present in the message being signed:

- o From, Reply-To, Resent-From
- o Subject
- o Date, Message-ID, Resent-Date, Resent-Message-ID
- o To, Cc, Resent-To, Resent-Cc
- o Content-Type, Content-ID, Content- Description)
- o List-Id, List-Help, List-Unsubscribe, List-Subscribe, List-Post, List-Owner, List-Archive

The following header fields SHOULD NOT be included in the signature:

- o Return-Path
- o Received
- o Comments, Keywords
- o Bcc, Resent-Bcc
- o Content-Signature (MUST NOT include)

Optional header fields (those not mentioned above) normally SHOULD NOT be included in the signature, due to the possibility of having additional header fields, of the same name, that are added or reordered legitimately, prior to verification. There are likely to be reasonable exceptions to this rule, given the wide variety of application-specific header fields that might be applied to a message, some of which are unlikely to be duplicated, modified, or reordered.

[4.](#) Considerations

[4.1.](#) Security Considerations

[4.2.](#) IANA Considerations

MIMEAUTH uses registries assigned to DOSETA [[I-D.DOSETA](#)]. This section specifies additions to these registries.

[4.2.1.](#) Content-Authentication Tag Specifications

These values are added to the registry that is now defined in [[I-D.DOSETA](#)]:

+-----+-----+-----+-----+-----+	
TYPE	REFERENCE
+-----+-----+-----+-----+-----+	
i	(this document, Section 3.1)
z	(this document, Section 3.1)
+-----+-----+-----+-----+-----+	

Table 1: Content-Authentication Tag Initial Values

[4.2.2.](#) Content-Authentication Header Field

IANA has added MIME Content-Authentication: to the "Permanent Message Header Fields" registry (see [[RFC3864](#)]) for the "mail" protocol, using this document as the reference.

[5.](#) References

[5.1.](#) Normative References

[[I-D.DOSETA](#)]

Crocker, D., Ed. and M. Kucherawy, Ed., "DomainKeys Security Tagging (DOSETA)",
I-D [draft-ietf-crocker-doseta-base](#), 2011.

[[RFC2045](#)] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", [RFC 2045](#), November 1996.

[[RFC2047](#)] Moore, K., "MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Content", [RFC 2047](#), November 1996.

[[RFC2119](#)] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", [RFC 4234](#), January 2008.

Internet-Draft

RFC4871bis

February 2011

[RFC5890] Klensin, J., "Internationalizing Domain Names in Applications (IDNA): Definitions and Document Framework", [RFC 5890](#), August 2010.

[5.2.](#) Informative References

[RFC1847] Galvin, J., Murphy, S., Crocker, S., and N. Freed, "Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted", [RFC 1847](#), October 1995.

[RFC3864] Klyne, G., Nottingham, M., and J. Mogul, "Registration Procedures for Message Header Fields", [BCP 90](#), [RFC 3864](#), September 2004.

[RFC4871] Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, "DomainKeys Identified Mail (DKIM) Signatures", [RFC 4871](#), May 2007.

[RFC4880] Callas, J., Donnerhacke, L., Finney, H., and R. Thayer, "OpenPGP Message Format", [RFC 4880](#), November 2007.

[Appendix A.](#) Acknowledgements

Authors' Addresses

D. Crocker
Brandenburg InternetWorking
675 Spruce Dr.
Sunnyvale
USA

Phone: +1.408.246.8253
Email: dcrocker@bbiw.net
URI: <http://bbiw.net>

M. Kucherawy

Cloudmark
128 King St., 2nd Floor
San Francisco, CA 94107
USA

Email: msk@cloudmark.com