

Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 04, 2014

A. Melnikov
Isode Ltd
July 03, 2013

**MMHS Draft and Release using S/MIME
draft-melnikov-mmhs-authorizing-users-00**

Abstract

This document describes a procedure for when an MMHS message is composed by one user and is only released to the mail transfer system when one or more authorizing users authorize release of the message by adding the MMHS-Authorizing-Users header field. The resulting message can be optionally countersigned, allowing recipients to verify both the original signature (if any) and countersignatures.

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 January 04, 2014.

Copyright Notice

Copyright (c) 2013 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 described in the Simplified BSD License.

Table of Contents

- [1.](#) Introduction [2](#)
- [2.](#) Conventions Used in This Document [2](#)
- [3.](#) Draft and Release procedure [3](#)
- [4.](#) MMHS-Authorizing-Users header field [4](#)
- [5.](#) Updated MIXER mapping [4](#)
 - [5.1.](#) Mapping from [RFC 5322](#)/MIME to X.400 [4](#)
 - [5.2.](#) Mapping from X.400 to [RFC 5322](#)/MIME [5](#)
- [6.](#) IANA Considerations [5](#)
- [7.](#) Security Considerations [5](#)
- [8.](#) Open Issues [5](#)
- [9.](#) References [6](#)
 - [9.1.](#) Normative References [6](#)
 - [9.2.](#) Informative References [6](#)
- [Appendix A.](#) Acknowledgements [6](#)

[1.](#) Introduction

In some secure environments email messages can't be released to the MTS (Mail Transfer System) and, thus delivered to recipients, unless they are authorized by one or more Releasing Officers. This document describes how this mechanism can be realized by an additional [[RFC5322](#)] header field and optionally using S/MIME [[RFC5750](#)] and [[RFC5751](#)].

This document describes a procedure for how an email message composed by one user can be released to the MTS when one or more authorizing users authorize and optionally countersign the message. The header communicates which users authorized the message. If signed, the resulting message allows recipients to verify both the original (if any) and counter S/MIME signatures. The list of authorizing users is specified in the MMHS-Authorizing-Users header field [Section 4](#). The original S/MIME signature generated by the sender (if any) should be unaffected by additional S/MIME countersignatures.

[2.](#) Conventions Used in This Document

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 [\[RFC2119\]](#).

The formal syntax uses the Augmented Backus-Naur Form (ABNF) [\[RFC5234\]](#) notation including the core rules defined in [Appendix B of RFC 5234](#) [\[RFC5234\]](#). Terms not defined in this document are taken from [\[RFC5322\]](#).

3. Draft and Release procedure

The original email message to be sent may or may not include sender's S/MIME signature. It doesn't include the MMHS-Authorizing-Users header field. `[[Is this true? Is there any use for specifying a value for the MMHS-Authorizing-Users header field before the message is countersigned?]]`

The document to be sent is first submitted over SMTP [\[RFC5322\]](#). The specific mechanism for how it arrives to authorizing user(s) is not specified in this document. One possibility is for the Submission MSA to redirect all email messages without the MMHS-Authorizing-Users header field and/or corresponding S/MIME countersignatures to a preconfigured mailbox that can be accessed by authorizing user(s).

Each user agent that is used by an authorized user has to perform the following steps:

1. Verify authenticity of the message. The exact mechanism to do that is out of scope for this document, but one example is by verifying the S/MIME signature and making sure that it matches the sender of the message, as described in [\[RFC5750\]](#) [\[RFC5751\]](#).
2. Check if the message already contains the MMHS-Authorizing-Users header field with the email address of the authorizing user. If yes, verify validity of the header field (for example by checking for S/MIME countersignature). If the validity of the MMHS-Authorizing-Users header field containing the email address of the authorizing user can be verified, go to step 5 below. Otherwise strip the MMHS-Authorizing-Users header field.

3. Allow the authorizing user to review content of the message. Some of the checks can be automated (for example search for keywords). If based on the check the authorizing user is happy to release the message to MTS (or to the next authorizing user, if multiple authorizations are required), the UA should optionally enable the authorizing user to add S/MIME countersignature. If the authorizing user wants to block the message, it can be discarded or returned to sender, and no further steps from this list should take place.
4. If there is an existing MMHS-Authorizing-Users header field containing the email address of the authorizing user, skip this step. Otherwise insert a new MMHS-Authorizing-Users header field (if absent) containing the email address of the authorizing user or append the email address of the authorizing user to the end of the existing MMHS-Authorizing-Users header field.
5. The (possibly) updated email message is either released to the MTS, or to the next authorizing user, as per email system configuration.

4. MMHS-Authorizing-Users header field

The MMHS-Authorizing-Users header field specifies the list of authorizing users that countersigned this email message (using S/MIME) before it was authorized for release to MTS. Each user is described by her/his email address.

The MMHS-Authorizing-Users header field specified in this document MUST NOT appear more than once in message headers.

```
MMHS-Authorizing-Users = "MMHS-Authorizing-Users:"  
                        [FWS] address-list [FWS] CRLF
```

```
address-list = <Defined in RFC 5322>
```

5. Updated MIXER mapping

This section updates MIXER mapping specified in [[RFC2156](#)].

5.1. Mapping from [RFC 5322](#)/MIME to X.400

In the absence of the MMHS-Authorizing-Users header field, From and Sender header fields are mapped to their X.400 equivalents as specified in [[RFC2156](#)].

If MMHS-Authorizing-Users header field is present:

1. The first From header field address is mapped to IPMS.Heading.originator if there is no Sender header field and the remaining From header field addresses + the MMHS-Authorizing-Users header field address(es) are mapped to IPMS.Heading.authorizing-users. If a Sender header field is present, the From header field address(es) and the MMHS-Authorizing-Users header field address(es) are mapped to IPMS.Heading.authorizing-users.
2. The Sender header field (if present) is mapped to IPMS.Heading.originator.

5.2. Mapping from X.400 to [RFC 5322](#)/MIME

Mapping from X.400 to Internet is controlled by whether or not a particular message is considered to be a military message. A message is considered to be a military message (as defined by ACP 123 [[ACP123](#)] and also specified in STANAG 4406 [[STANAG-4406](#)]) if there are any MMHS heading extensions present. Alternatively, this MAY be done by configuration (i.e. all messages can be considered to be military messages).

For non military messages, mapping from X.400 as specified in [[RFC2156](#)] is used.

For military messages, the following mapping is used:

1. IPMS.Heading.originator is mapped to From header field.
2. The IPMS.Heading.authorizing-users is mapped to MMHS-Authorizing-Users header field.

6. IANA Considerations

IANA is requested to add the MMHS-Authorizing-Users header field specified in [Section 4](#) to the "Permanent Message Header Field Registry", defined by Registration Procedures for Message Header Fields [[RFC3864](#)].

7. Security Considerations

TBD

8. Open Issues

Netnews Approved header field has the same syntax and semantics as the one described here. Should it be used (and be formally registered for email) instead?

Allow use of MMHS-Authorized-Users/Approved for specifying who should authorize release of the message (as opposed to just for recording of who authorized release so far)?

9. References

9.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC2156] Kille, S., "MIXER (Mime Internet X.400 Enhanced Relay): Mapping between X.400 and [RFC 822](#)/MIME", [RFC 2156](#), January 1998.
- [RFC5322] Resnick, P., Ed., "Internet Message Format", [RFC 5322](#), October 2008.
- [RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, [RFC 5234](#), January 2008.
- [RFC5750] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Certificate Handling", [RFC 5750](#), January 2010.
- [RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", [RFC 5751](#), January 2010.
- [ACP123] CCEB, ., "Common Messaging strategy and procedures", ACP 123, May 2009.

9.2. Informative References

- [RFC3864] Klyne, G., Nottingham, M., and J. Mogul, "Registration Procedures for Message Header Fields", [BCP 90](#), [RFC 3864](#), September 2004.
- [STANAG-4406] NATO, ., "STANAG 4406 Edition 2: Military Message Handling System", STANAG 4406, March 2005.

Appendix A. Acknowledgements

Many thanks for reviews and text provided by Steve Kille and David Wilson.

Author's Address

Alexey Melnikov
Isode Ltd
5 Castle Business Village
36 Station Road
Hampton, Middlesex TW12 2BX
UK

E-Mail: Alexey.Melnikov@isode.com

