

openpgp
Internet-Draft
Intended status: Informational
Expires: 18 October 2025

B. R. Einarsson
Mailpile ehf
juga
Independent
D. K. Gillmor
ACLU
16 April 2025

(Deprecated) Protected E-mail Headers
draft-autocrypt-lamps-protected-headers-03

Abstract

This is a tombstone document of an abandoned effort to provide end-to-end cryptographic protections for e-mail headers. It has been superseded by draft-ietf-lamps-header-protection

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 <https://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 18 October 2025.

Copyright Notice

Copyright (c) 2025 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 (<https://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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. This Document Is Deprecated	2
2. References	2
2.1. Normative References	2
2.2. Informative References	2
Appendix A. Document Considerations	2
A.1. Document History	3
Appendix B. Acknowledgements	3
Authors' Addresses	4

1. This Document Is Deprecated

This document has been superseded by
[I-D.ietf-lamps-header-protection].

2. References

2.1. Normative References

[I-D.ietf-lamps-header-protection]

Gillmor, D. K., Hoeneisen, B., and A. Melnikov, "Header Protection for Cryptographically Protected E-mail", Work in Progress, Internet-Draft, draft-ietf-lamps-header-protection-25, 6 January 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-lamps-header-protection-25>>.

2.2. Informative References

[Autocrypt]

"Autocrypt Specification 1.1", 13 October 2019, <<https://autocrypt.org/level1.html>>.

[OpenPGP-Email-Summit-2019]

"OpenPGP Email Summit 2019", 13 October 2019, <<https://wiki.gnupg.org/OpenPGPEmailSummit201910>>.

[xkcd936] Munroe, R., "xkcd: Password Strength", 10 August 2011, <<https://www.xkcd.com/936/>>.

Appendix A. Document Considerations

[RFC Editor: please remove this section before publication]

This document is currently edited as markdown. Minor editorial changes can be suggested via merge requests at <https://github.com/autocrypt/protected-headers> or by e-mail to the authors. Please direct all significant commentary to the public IETF LAMPS mailing list: spasm@ietf.org

A.1. Document History

Significant changes between version -02 and -03:

- * "Tombstone" this document in favor of draft-ietf-lamps-header-protection

Significant changes between version -01 and -02:

- * Added S/MIME test vectors in addition to PGP/MIME
- * Legacy Display parts should now be text/plain and not text/rfc822-headers
- * Cryptographic Payload must have protected-headers parameter set to v1
- * Test vector sample Message-Ids have been normalized
- * Added encrypted-only (unsigned) test vectors, at the suggestion of Russ Housley

Changes between version -00 and -01:

- * Credit Randall for "correct horse battery staple".
- * Adjust test vectors to ensure no line in the generated .txt format exceeds 72 chars.
- * Minor formatting cleanup to appease idnits.
- * Update references to more recent documents (RFC 2822 -> 5322, -00 to -01 of draft-ietf-lamps-header-protection-requirements).

Appendix B. Acknowledgements

The set of constructs and algorithms in this document has a previous working title of "Memory Hole", but that title is no longer used as different implementations gained experience in working with it.

These ideas were tested and fine-tuned in part by the loose collaboration of MUA developers known as [Autocrypt].

Additional feedback and useful guidance was contributed by attendees of the OpenPGP e-mail summit ([OpenPGP-Email-Summit-2019]).

The following people have contributed implementation experience, documentation, critique, and other feedback:

- * Holger Krekel
- * Patrick Brunschwig
- * Vincent Breitmoser
- * Edwin Taylor
- * Alexey Melnikov
- * Russ Housley

The password example used in previous versions comes from [xkcd936].

Authors' Addresses

Bjarni Rannar Einarsson
Mailpile ehf
Baronsstigur
Iceland
Email: bre@mailpile.is

juga
Independent
Email: juga@riseup.net

Daniel Kahn Gillmor
American Civil Liberties Union
125 Broad St.
New York, NY, 10004
United States of America
Email: dkg@fifthhorseman.net