Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 19, 2015

T. Bray, Ed.
Textuality

October 16, 2014

The OpenPGP Message Format
draft-bray-pgp-message-00

Abstract

RFC 4880 specifies the encoding for encrypted OpenPGP messages. This document registers an Internet Media Type for these messages.

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 April 19, 2015.

Copyright Notice

Table of Contents

1. Introduction

The OpenPGP message format, specified in [RFC4880], is widely supported, with implementations in many programming languages.

[RFC3156] specifies the "multipart/encrypted" media type to describe these messages; the "application/pgp-encrypted", "application/pgp-signature", and "application/pgp-keys" media types are specified for use as protocol parameter values and the content type of the MIME body parts.

Currently, there exist popular applications which specialize in the interchange of pure text payloads. These can be used for the transport of OpenPGP messages (perhaps on a copy-and-paste basis), but they typically do not support multipart messages and thus would have difficulty with RFC3156-style packaging. It would be advantageous if these "naked" OpenPGP messages could be labeled with a media type to facilitate dispatch to software which can decrypt them.

1.1. 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 grammatical rules in this document are to be interpreted as described in [RFC5234].

2. OpenPGP Message

The format of OpenPGP Messages is described in [RFC4880]. Messages can be encoded in one of two formats: binary (section 11.3) or textual "ASCII-armored" (sections 2.4 and 6).

A single media type serves to identify both, since they are trivially distinguishable.

A binary message is a sequence of "packets", each of which has a header (see section 4 of RFC4880) beginning with a "tag" byte, which must have the high-order bit set.

The syntax of an ASCII-armored message is specified in detail in RFC4880 Section 6. This specification will not create ABNF to replicate that specification, since it is widely understood and there are many successful software implementations which consume it. However, it begins with a leading hyphen ("-", U+002D HYPHEN-MINUS).

For flexibiity and better support of copy/paste operation, this specification alows the body of an application/pgp-message to have insignificant white space ("ws" in the production below) surrounding the ASCII-Armored form of the message. Popular implementations are observed to ignore such white space.

```
ws = *(
        %x20 /              ; Space
        %x09 /              ; Horizontal tab
        %x0A /              ; Line feed or New line
        %x0D )              ; Carriage return
```

Thus, software receiving a message labeled with the application/pgp-message media type can straightforwardly decide how to parse it. If the high-order bit of the first byte is set, then such software MUST attempt to parse it as a binary OpenPGP message as specified in RFC4880 section 11.3. Otherwise, if the first byte is a hyphen, or matches the "ws" production above, such software MUST attempt to parse it as an ASCII-Armored OpenPGP message as specified in RFC4880 section 6. If the first byte meets neither condition, the payload is malformed and no parsing is possible.

3. IANA Considerations

The MIME media type for an OpenPGP Message is application/pgp-message.

Type name: application

Subtype name: pgp-message

Required parameters: n/a

Optional parameters: n/a

Encoding considerations: binary

Security considerations: This document.

Interoperability considerations: Described in this document

Published specification: This document

Additional information: Magic number(s): n/a
File extension(s): .asc for ASCII-armored, none for binary
Macintosh file type code(s): TEXT

Person & email address to contact for further information: IESG
<iesg@ietf.org>

Intended usage: COMMON

Restrictions on usage: none

Author: Tim Bray
<tbray@textuality.com>

Change controller: IESG
<iesg@ietf.org>

4. Security Considerations

The presence of an OpenPGP message serves as notice that the sender (and probably the receiver) have a strong desire to keep its contents private. It is widely believed that messages encoded using modern cryptography are extremely difficult for an adversary to decrypt. Therefore, adversaries typically focus their attacks on end-point software that may inadvertantly expose either the decryption key or the payload of the message.

It is therefore RECOMMENDED that software which recognizes the application/pgp media type dispatch the encrypted payload as-is to other software which is known to be trusted by the user for purposes of decryption. It is further RECOMMENDED that software which recognizes the application/pgp-message media type actively try to avoid storing the decrypted form of such messages or the keys used for decryption, and furthermore actively avoid providing the user interface used for interaction with the decryption software.

Implementers should also consult and pay careful attention to the Security Considerations section of RFC4880.

5. Interoperability Considerations

RFC4880 notes that implementations SHOULD support the ASCII-Armored representation of OpenPGP messages; this format has proven reasonably resiliant to damage during transition over a variety of network channels and, while it occupies more bytes of storage, is often preferred for interchange over general-purpose messaging channels.

6. Example

This is an ASCII-Armored OpenPGP Message:

```
-----BEGIN PGP MESSAGE-----
Version: OpenPrivacy 0.99

yDgBO22WxBHv7O8X7O/jygAEzol56iUKiXmV+XmpCtmpqQUKiQrFqclFqUDBovzS
vBSFjNSiVHsuAA==
=njUN
-----END PGP MESSAGE-----
```

7. Normative References

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

[RFC3156] Elkins, M., Del Torto, D., Levien, R., and T. Roessler, "MIME Security with OpenPGP", RFC 3156, August 2001.

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

[RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

Author's Address

Tim Bray (editor)
Textuality

Email: tbray@textuality.com