Internet Engineering Task Force	V.M. Moscaritolo, Ed.
Internet-Draft	PGP, part of Symantec Corporation
Intended status: Informational	April 08, 2011
Expires: October 10, 2011	

Media type literal packet in OpenPGP
draft-moscaritolo-openpgp-literal-01

Abstract

This document describes an extension to the OpenPGP Message Format that allows a Internet Media Type to be associated with the encoded content. By providing more information beyond the existing binary and text formats this extension can enable the automated selection of an appropriate media viewer for the decoded content.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

This document describes an extension to the OpenPGP Message Format that allows a Internet Media Type (aka RFC-2046 MIME type) to be associated with the encoded content. By providing more information beyond the existing binary and text formats this extension and can enable the automated selection of an appropriate media viewer for the decoded content.

2. Terms

*OpenPGP - This is a term for security software that uses PGP 5.x as a basis, formalized in RFC 4880 *[RFC4880]*.

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 RFC 2119 *[RFC2119]*.

3. Literal Data packet

The OpenPGP RFC 4880 *[RFC4880]* currently specifies only a few formats for encoded content: text, binary and UTF-8. The format itself of the content is specified in section 5.9 as part of the Literal Data packet (Tag 11). In addition to the body of the message being encoded, this packet also contains a one-octet field that describes how the data is formatted.
The current choices are 'b' (0x62), in which case the Literal packet contains binary data and 't' (0x74) which describes text data and 'u' (0x75) for UTF-8 Data.

This field is followed by a file name as a string (one-octet length, followed by a file name). While not detailed in the RFC, most implementations of PGP also add a trailing null at the end of the file name but use the string length to skip to the next field.
We propose to add a new formatting type of 'm' (0x6d) to describe that there is a RFC 2046 *[RFC2046]* Internet media type associated with the literal data. In the case of a 'm' format type, the media type is appended to the end of the null terminated file name, while extending the file name length byte to accommodate this additional information.

4. Example of literal packet taged with a media type

```
0000 6d 17 73 6f 6d 65 64 61 74 61 2e 6a 70 67 00 69 |m.somedata.jpg.i|
0010 6d 61 67 65 2f 6a 70 65 67                      |mage/jpeg       |
```

The following is an example of a Literal Data packet (Tag 11) that specifies the media type format image/jpeg for a file named 'somedata.jpg'

5. OpenPGP Implementation Considerations.

OpenPGP implementations supporting the media literal data packet format SHOULD use the media type string to select the appropriate viewer for the encoded content. Implementations should consider the following possibilities: RFC 4880 *[RFC4880]* section 13.10.

- As with the existing file name field, the string length can be zero bytes long, indicating that there is no file name or media type specified.

- There might be no null byte at the end of the file name, or no additional bytes specified in the file name string length, indicating that there is no media type specified.

- The file string could have bytes specified but start with a null byte, this indicates that no file name is specified but that this is a media type associated with the content.

- The media type MAY have an OPTIONAL null byte termination. Any data that follows such a null byte should be discarded and not considered part of the media type.

- While the one-octet length of the file name field does limit the combined length of suggested file name and media type, it does allow for some reasonable usage. In the case of combined length of suggested file name and media type string that exceeds 255 bytes, priority should be given to the media type string, and truncation of the filename is suggested. if such truncation

should occur it is suggested that the file name extension be preserved.

In the long run, a more correct method of associated media type with content might employ one of the experimental tags mentioned in

6. Acknowledgements

The author would like to acknowledge the help of many individuals who helped in particular Derek Atkins, Jon Callas, David Shaw, Damon Cokenias, David Finkelstein, Hal Finney and Will Price.

7. Contributors

Damon Cokenias, David Shaw, Derek Atkins and Jon Callas provided important criticism on compliance with OpenPGP RFC 4880 *[RFC4880]*.

8. IANA Considerations

This memo includes no request to IANA.

9. Security Considerations

*The addition of a media type string increases the possibility of truncation of a large file name field in the Literal Packet.

*The addition of media type string after the file name string null termination does not add any hidden channels that didn't potentially exist in the OpenPGP protocol.

*Since the signature hash of an RFC 4880 *[RFC4880]* OpenPGP message does not cover the literal packet metadata, it is possible for an attacker to modify both the filename and format field without invalidating the signature. When using this media type extension there is a possibility that an attacker to force a particular content handler to run on the decoding implementation.

*In order to prevent modification of the media type, encrypting and encapsulating the Literal Data packet using the Symmetrically Encrypted Integrity Protected Data Packet (Tag 18) as specified in OpenPGP RFC 4880 *[RFC4880]* is highly recommended.

10. References

10.1. Normative References

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
[RFC4880]	

	Callas, J., Donnerhacke, L., Finney, H., Shaw, D. and R. Thayer, "OpenPGP Message Format", RFC 4880, November 2007.
[RFC2046]	Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", RFC 2046, November 1996.

10.2. Informative References

[RFC2629]	Rose, M.T., "Writing I-Ds and RFCs using XML", RFC 2629, June 1999.
[RFC3552]	Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, July 2003.
[I-D.narten-iana-considerations-rfc2434bis]	Narten, T and H Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", Internet-Draft draft-narten-iana-considerations-rfc2434bis-09, March 2008.

Author's Address

Vinnie Moscaritolo editor Moscaritolo PGP, part of Symantec Corporation Mountain View, CA US EMail: vinnie@pgp.com