```
Network Working Group          N. Borenstein, First Virtual
Internet Draft                                     C. Plumb
Category: Informational                      P. Zimmermann
                               Boulder Software Engineering
                                                   May 1994
```


The application/pgp MIME Content-type

Status of this Memo

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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.’’

To learn the current status of any Internet-Draft, please check the ‘‘1id-abstracts.txt’’ listing contained in the Internet-Drafts Shadow Directories on ds.internic.net (US East Coast), nic.nordu.net (Europe), ftp.isi.edu (US West Coast), or munnari.oz.au (Pacific Rim).

Abstract

MIME [RFC-1341, RFC-1521] defines a format and general framework for the representation of a wide variety of data types in Internet mail. This document defines one particular type of MIME data, the application/pgp type, for "pretty good" privacy, authentication, and encryption in Internet mail. The application/pgp MIME type is intended to facilitate the wider interoperation of private mail across a wide variety of hardware and software platforms.

The application/pgp MIME type

This document defines an extremely simple subtype of the MIME content-type "application", the "application/pgp" subtype. This subtype was designed to meet the following criteria:

1. Maximal backward-compatibility with pre-MIME implementations of PGP for ASCII text mail.

2. Ability to use PGP to enhance the privacy of MIME mail with non-ASCII or non-text data.

3. Ability to optionally differentiate "key-only" messages from more complex PGP data, for different treatment by user agent software

4. Ease of implementation.

This document defines a new MIME content-type, "application/pgp". The content-type line for this type may have one optional parameters, "format", as described below.

The MIME content-type "application/pgp" is a very simple adaptation of PGP. When a MIME entity has a content-type of "application/pgp", the data within it is assumed to be in PGP format. [PGP]

PGP's data format is ASCII text that includes blocks of privacy-enhanced text. Such text might be authenticated (signed), or encrypted. The PGP data is self-describing with regard to format and content. In current versions of PGP, only textual data can be encrypted. Beginning with a future version of PGP, it is expected that arbitrary MIME data can also be encrypted, but the fact that the data is in MIME format is not evident from the outside of the PGP data. Thus even the content-type of data being transmitted may be made private by PGP.

Of course, once any decryption or verification is performed, the resulting data must be displayed to the user. A future version of PGP will include a command line option that will guarantee that ALL output will be in MIME format, regardless of whether it was initially encrypted as MIME or text. With this option, the decrypted result of any application/pgp MIME entity may be used as input to any general-purpose MIME-viewing tool.

The "Format" Parameter

The optional parameter "format" may be included on the Content-line for PGP data, to declare the type of encrypted data enclosed, as follows:

```
Content-type: application/pgp; format=mime
```

or

```
Content-type: application/pgp; format=keys-only
```

or

```
Content-type: application/pgp; format=text
```

This memo defines only three possible values for the format parameter, namely "text", "mime", and "keys-only".

It should be stressed that the format parameter is completely optional. Further, it is expected that a future release of PGP will make this parameter completely unnecessary for any desired functionality, by building knowledge about encapsulated MIME into the PGP data structures. However, the parameter may remain a convenience for some implementors, and in the interim the "format=mime" parameter makes it possible for existing MIME and PGP implementations to be configured to interoperate smoothly for the automatic encryption and decryption of non-textual data. In the absence of the "format" parameter, the decrypted data from non-MIME-aware versions of PGP should generally be treated as ASCII text by mail readers.

Format=text

If present, the parameter "format=text" indicates that the result of decrypting the application/pgp entity is textual data, including data encrypted by pre-MIME versions of PGP. No further MIME-related processing is called for after decryption.

Text is the default value of the format parameter. That is, the following two Content-type specifications should be treated as equivalent by user agents:

```
Content-type: application/pgp
Content-type: application/pgp; format=text
```

However, it should be noted that the latter form is more explicit, and should be generated whenever an encrypting agent has definite knowledge that the data being encrypted are simply non-MIME text.

Format=mime

If present, the parameter "format=mime" indicates that the result of decrypting the application/pgp entity should be treated as another MIME entity. That is, it should be inspected for Content-type, etc. and parsed recursively as a MIME entity.

Format=keys-only

If present, the parameter "format=keys-only" indicates that the application/pgp entity contains no encrypted or other data, only PGP keys. A user agent that so chooses may treat such entities specially, e.g. by providing the user with a special key-management interface. A user agent without such specialized understanding may ignore the "keys-only" parameter, and (for example) pass all "application/pgp" entities directly to the pgp program.

A Note on Transfer Encodings

One area where MIME and PGP have redundant mechanisms is in the transformation of binary data into a mail-safe form. For this purpose, PGP uses "ASCII armor" and MIME uses the base64 content-transfer-encoding. As it happens, these mechanisms are virtually identical, but are flagged in different manners. The PGP mechanism is self-identifying, while the MIME mechanism uses a "Content-Transfer-Encoding" header field.

The application/pgp content-type has been carefully designed to let either of these mechanisms be used. If PGP is used in a manner that produces "ASCII armor", then no MIME content-transfer-encoding is needed (or "7bit" may be used). If PGP is used in a manner that produces binary data, then a MIME content-transfer-encoding of "base64" may be used, and a MIME agent will restore the data to its binary form before processing it as PGP data.

This duality of mechanisms implies, however, that the PGP-processing routines must be prepared to receive PGP data in either binary OR ASCII armor forms.

Security Considerations

Security issues are not discussed in this memo, which only describes how PGP usage is labelled in MIME. PGP itself, of course, is a technology focused on issues of security and privacy, and the PGP documentation is replete with helpful information and advice about the security issues PGP seeks to address.

Authors' Addresses

For more information, the author of this document may be contacted via Internet mail:

Nathaniel S. Borenstein
First Virtual Holdings
25 Washington Avenue
Morristown, NJ 07960 USA
Email: nsb@nsb.fv.com
Phone: +1 201 540 8967
Fax: +1 201 993 3032

Colin Plumb
43 Farnham Ave.
Toronto, Ontario M4V 1H6 Canada

Email: colin@nyx.cs.du.edu
Phone: +1 416 968 1261

Philip Zimmermann
3021 11th Street
Boulder, Colorado 80304 USA
Email: prz@acm.org
Phone: +1 303 541 0140

Acknowledgements

The authors wish to thank Derek Atkins for his helpful comments on earlier drafts of this memo.

<<Need to fill in others????>>

References

[RFC-1341] Borenstein, N., and N. Freed, "MIME (Multipurpose Internet Mail Extensions): Mechanisms for Specifying and Describing the Format of Internet Message Bodies", RFC 1341, Bellcore, Innosoft, June, 1992.

[RFC-1521] Borenstein, N., and N. Freed, "MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies", RFC 1521, Bellcore, Innosoft, September, 1993.

[PGP] ****NEED TO FILL IN ****

Table of Contents