Network Working Group
Internet-Draft
Intended status: Informational
Expires: March 1, 2015

A. Smasher
S. Josefsson

August 28, 2014

The "OpenPGP" mail and news header field
draft-josefsson-openpgp-mailnews-header-07

Abstract

This document describes the "OpenPGP" mail and news header field. The field provide information about the sender's OpenPGP key.

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 March 1, 2015.

Copyright Notice

Table of Contents

1. Preface

This document define the "OpenPGP" message header field. This field is suitable for both mail [RFC5322] and netnews [RFC1036] messages, and is used to provide information about the sender's OpenPGP [RFC4880] key.

This document should be interpreted within the context of [RFC5322]. In the event of a discrepancy, refer to that 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 RFC 2119 [RFC2119].

2. Background and Motivation

There are quite a few PGP and GnuPG users who add header fields with information about the sender's OpenPGP key. Fields in current use include "X-PGP:", "X-PGP-Key:", "X-Request-PGP:", "X-PGP-KeyID:", and "X-PGP-Fingerprint:". The fields are not standardized, so they cannot be reliably parsed automatically by applications, only parsed by humans.

Since both PGP and GnuPG rely on the OpenPGP protocol, it appears preferable to use the term "OpenPGP" rather than "PGP", or "GPG", in the field name. The latter forms appear as underhanded attempts to advocate specific applications, rather than the open standard they both share. The field specified here is named "OpenPGP".

The OpenPGP field is not a required part of successful use of OpenPGP in e-mail or other messages. It is intended as a convenience, in those situations where the user experience may be enhanced by using the information in the field. Consequently, the information in the field should not disrupt the normal OpenPGP key retrieval and web of trust mechanism. Neither the integrity nor the authenticity of the information in the field should be assumed to be correct or trust-worthy.

This document neither suggests a specific scenario of when the field should be used, nor how it should be used. It is acknowledged that the dominant use of the information in the field may be by humans and not applications.

To promote good use of the field, care should be taken so that applications do not trigger error messages that may annoy the user, when an error condition arises during handling of the OpenPGP field. It is generally recommended that an implementation ignore the

presence of an OpenPGP field if it would cause an error condition. Since the field is optional, this approach should not be difficult to implement. The philosophy here is to enable an enhanced user experience. Error messages rarely contribute to that goal.

3. OpenPGP Header Field

The OpenPGP header field is intended to present characteristics of the sender's OpenPGP key. The field typically contains the Key ID and the URL where the key can be retrieved.

Because the mail header is typically not integrity protected, the information conveyed in the OpenPGP header field MUST NOT be trusted without additional verification. Some of the information given in this field may also be given in the OpenPGP key itself. When these two sources conflict, users SHOULD favor the information from the OpenPGP key, as that information can be cryptographically protected.

The field is of a "structured" type (see section 2.2.2 of RFC 5322). In general, the structure consist of one or more parameters, each consisting of one attribute and one value. The terminology and format of the field was inspired by MIME [RFC2045]. The various provisions of RFC 2045 apply. In particular, the value part of parameters may be quoted; whitespace, folding and comments may occur in the middle of parameters; except as noted below.

The OpenPGP header field is defined below in the Augmented BNF [RFC5234] notation. By itself, however, this grammar is incomplete. It refers by name to syntax rules that are defined in [RFC5322] and [RFC3986]. Rather than reproduce those definitions here, and risk unintentional differences between the two, this document refers the reader to the other documents for the definition of non-terminals.

Implementations MUST understand the "id", "url", and "preference" attributes. Parameter with unrecognized attributes MUST be ignored. The grammar permits unknown parameters to allow for future extensions. Each parameter attribute (e.g., "url") MUST NOT occur more than once in any single instance of the OpenPGP field. The OpenPGP field itself MAY occur more than once in a single email (for example if the sender has multiple keys).

```
   openpgp     = "OpenPGP:" o-params CRLF
                   ; CFWS is defined in RFC 5322.
                   ; CRLF is defined in RFC 5234.

   o-params    = (o-parameter *(";" o-parameter))

   o-parameter = *CFWS "id" "=" id *CFWS
               / *CFWS "url" "=" url *CFWS
               / *CFWS "preference" "=" preference *CFWS
               / *CFWS parameter *CFWS ; normally unused, for extensions
                   ; parameter is defined in RFC 2045.

   id          = 1*(8HEXDIG)
                   ; HEXDIG is defined in RFC 5234.
                   ; Matching of value is case-insensitive.

   url         = folded-uri / quoted-url
                   ; If the URL contains the character ";",
                   ; the quoted-url form MUST be used.

   quoted-url  = DQUOTE folded-uri DQUOTE
                   ; DQUOTE is defined in RFC 5234.

   folded-uri  = <absolute-URI, but free insertion of FWS permitted>
                   ; absoluteURI is defined in RFC 3986.
                   ; FWS is defined in RFC 5234.

   preference  = "sign" / "encrypt" / "signencrypt" / "unprotected"
                   ; Matching of values is case-insensitive.
```

The folded-URI MAY contain folding whitespace (FWS, [RFC5322]), which is ignored. To convert a folded-URI to a absolute-URI, first apply standard [RFC5322] unfolding rules (replacing FWS with a single SP), and then delete any remaining un-encoded SP characters. Folding may be used to shorten long lines.

3.1. Primary Key ID field: id

The "id" parameter, if present, MUST hold the Key ID or key fingerprint for the primary key. The value uses the hex [RFC4648] notation. The parameter value is case-insensitive.

The length of the field determines whether it denotes a Key ID (8 hex symbols), a long Key ID (16 hex symbols), a v3 key fingerprint (32 hex symbols), or a v4 key fingerprint (40 hex symbols).

Note that each of the following examples includes a comment, which is optional.

```
id=12345678 (short key ID)
id=1234567890ABCDEF (long key ID)
id=1234567890abcdef0123456789ABCDEF01234567 (v4 fingerprint)
id=1234567890ABCDEF0123456789ABCDEF (v3 fingerprint, deprecated)
```

3.2. Key URL field: url

The "url" parameter, if present, MUST specify a URL where the public key can be found. It is RECOMMENDED to use a common URL family, such as HTTP [RFC2616] or FTP [RFC0959]. The URL MUST be fully qualified, MUST explicitly specify a protocol and SHOULD be accessible on the public Internet.

The content of where the URL points SHOULD be either an ASCII armored or binary OpenPGP packet containing the key. A valid reason for storing something else may be if the key has been revoked.

For example:

```
url=http://example.org/pgp.txt
url="http://example.org/funny;name.txt"
```

If the URL contains the character ';' the entire URL MUST be quoted, as illustrated in the example.

3.3. Protection Preference Field: preference

The "preference" parameter, if present, specify the quality of protection preferred by the sender. The parameter value is case-insensitive.

The available values are as follows. The "unprotected" token means that the sender prefers not to receive OpenPGP protected e-mails. The "sign" token means that the sender prefers to receive digitally signed e-mails. The "encrypt" token means that the sender prefers to receive encrypted e-mails. A "signencrypt" token means that the sender prefers to receive encrypted and signed e-mails.

Note that there is no normative requirement on the receiver to follow the stated preference.

For example:

```
preference=sign
preference=unprotected
preference=ENCRYPT
```

4. Comments

As discussed in section 3.2.2 of RFC 5322, comments may appear in header field bodies. Comments are not intended to be interpreted by any application, but to provide additional information for humans.

The following are examples of OpenPGP fields with comments:

```
id=B565716F (key stored on non-networked laptop)
id=12345678 (1024 bit RSA Key for Encrypt or Sign)
id=ABCD0123 (created Sun Jan  2 02:25:15 CET 2005)
```

5. Examples

These are valid examples of how the field may be used. This list is not meant to be exhaustive, but to reflect expected typical usages.

```
OpenPGP: id=12345678
OpenPGP: url=http://example.com/key.txt
OpenPGP: preference=unprotected
OpenPGP: url=http://example.com/key.txt; id=12345678
OpenPGP: id=12345678; url=http://example.com/key.txt;
         preference=signencrypt
OpenPGP: url=http://example.com/key.txt (down 2-3pm UTC);
         id=12345678 (this key is only used at the office);
         preference=sign (unsigned emails are filtered away)
OpenPGP: id=12345678; url="http://example.com/openpgp;key.txt"
```

6. Acknowledgements

The content of this document builds on discussions with (in alphabetical order) Christian Biere, Patrick Brunschwig, Jon Callas, Dave Evans, Alfred Hoenes, Peter J. Holzer, Ingo Klocker, Werner Koch, Jochen Kupper, William Leibzon, Charles Lindsey, Aleksandar Milivojevic, Xavier Maillard, Greg Sabino Mullane, Tim Polk, Thomas Roessler, Moritz Schulte, Olav Seyfarth, David Shaw, Thomas Sjogren, Paul Walker, and Steve Youngs. No doubt the list is incomplete. We apologize to anyone we left out.

7. Security Considerations

The OpenPGP header field is intended to be a convenience in locating public keys; it is neither secure nor intended to be. Since the message header is easy to spoof, information contained in the header should not be trusted. The information must be verified.

Applications that interpret the field MUST NOT assume that the content is correct, and MUST NOT present the data to the user in any way that would cause the user to assume that it is correct. Applications that interpret the data within the field SHOULD alert the user that this information is not a substitute for personally verifying keys and being a part of the web of trust.

If an application receives a signed message and uses the information in the field to automatically retrieve a key, the application MAY ignore the retrieved key if it is not the same key used to sign the message. This SHOULD be done before the newly retrieved key is imported into the user's keyring.

The use of HTTPS [RFC2818], DNSSEC [RFC4033], SMTP STARTTLS [RFC3207], IMAP/POP3 STARTTLS [RFC2595] and other secure protocols, may enhance the security of information conveyed through this field, but does not guarantee any level of security or authenticity. Developers and users must remain aware of this.

Version 3 OpenPGP keys can be created with a chosen key id (aka "the 0xDEADBEEF attack"). Verifying the Key ID of a retrieved key against the one provided in the field is thus not sufficient to protect against a man-in-the-middle attack. Instead, the web-of-trust mechanism should be used.

If an attacker wants to check the validity of email addresses, he might email arbitrary addresses with a unique OpenPGP header field URL (presumably an URL under the attacker's control). The attacker can verify the liveness of each email address by checking if the URL for each particular recipient has been retrieved. To protect against this, implementations MUST inform the user of that potential privacy issue when retrieving keys from an URL provided by the field of an inbound email message: either when the feature is enabled or to be used for the first time or every time the MUA detects an unknown key.

Given the flexibility of the syntax of the field, slightly varying the content between messages can be used as a covert channel. This is already possible using other header fields in email, and thus the OpenPGP field does not introduce a new vulnerability here.

8. IANA Considerations

The IANA is asked to register the OpenPGP header field, using the template as follows, in accordance with RFC 3864 [RFC3864].

Header field name: OpenPGP

Applicable protocol: mail, netnews

Status: informational

Author/Change controller: IETF

Specification document(s): This document.

Related information: None

9. References

9.1. Normative References

[RFC2045] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996.

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

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

[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.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, October 2008.

9.2. Informative References

[RFC0959] Postel, J. and J. Reynolds, "File Transfer Protocol", STD 9, RFC 959, October 1985.

[RFC1036] Horton, M. and R. Adams, "Standard for interchange of USENET messages", RFC 1036, December 1987.

[RFC2595] Newman, C., "Using TLS with IMAP, POP3 and ACAP", RFC 2595, June 1999.

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000.

[RFC3207] Hoffman, P., "SMTP Service Extension for Secure SMTP over Transport Layer Security", RFC 3207, February 2002.

[RFC3864] Klyne, G., Nottingham, M., and J. Mogul, "Registration Procedures for Message Header Fields", BCP 90, RFC 3864, September 2004.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, October 2006.

Appendix A. Copying conditions

Authors' Addresses

Atom Smasher

Email: atom@smasher.org (762A3B98A3C396C9C6B7582AB88D52E4D9F57808)

Simon Josefsson

Email: simon@josefsson.org (9AA9BDB11BB1B99A21285A330664A76954265E8C)