Internet-Draft
OpenPGP Working Group
draft-ietf-openpgp-multsig-01.txt

D. Del Torto
CryptoRights Foundation
R. Levien
University of California at Berkeley
T. Roessler

August 2000

Multiple Signatures using Security Multiparts

Status of this Memo

Abstract

This document describes how the Security Multiparts defined in RFC 1847 [1] can be used to transport multiple digital signatures.

This draft is being discussed on the "ietf-openpgp" mailing list. To join the list, send a message to <ietf-openpgp-request@imc.org> with the single word "subscribe" in the subject. A web site containing an archive of the list can be found at <http://www.imc.org/ietf-openpgp>.

1. Introduction

Various digital signature services for electronic mail rely on the framework defined in RFC 1847. These signature services do not address the issue of parallel signatures on the same content.

Instead of specifying parallel signature formats for individual signature services such as OpenPGP, the present document defines a "multipart/mixed" protocol for the "multipart/signed" body type introduced in RFC 1847. The "multipart/mixed" protocol permits users to bundle parallel signatures for the same content into one "multipart/signed" body part. It is independent of the protocols used to form the individual digital signatures.

1.1. Compliance

In order for an implementation to be compliant with this specification, is it absolutely necessary for it to obey all items labeled as MUST or REQUIRED.

2. The "multipart/mixed" protocol

2.1. Specification

Digitally signed messages conforming to this document are denoted by the "multipart/signed" content type, defined in RFC 1847, with a "protocol" parameter which MUST have a value of "multipart/mixed". (MUST be quoted).

The "micalg" parameter MUST contain a comma-separated list of hash-symbols. These hash-symbols identify the message integrity check (MIC) algorithm(s) used to generate the subsequent signature(s). Hash-symbols MUST NOT occur more than once in this list.

The multipart/signed body MUST consist of exactly two parts. The first part contains the signed data in MIME canonical format, including a set of appropriate content headers describing the data.

The second part MUST be of type "multipart/mixed". Each sub-part represents an individual digital signature which has been formed according to RFC 1847 and the specification of the signature protocol used.

2.2. Example message

```
From: Dave Del Torto <ddt@openpgp.net>
To: Raph Levien <raph@acm.org>
Mime-Version: 1.0
Content-Type: multipart/signed; protocol="multipart/mixed";
   boundary=0000_031; micalg="pgp-sha1, rsa-md5, pgp-md5"

--0000_031
Content-Type: text/plain

Hi Raph,

Here's some text with parallel (multiple) digital signatures
in various formats.

   dave


-------------------------------------------------------------------------
"All email luxuriantly hand-crafted using only the finest ASCII text."

--0000_031
Content-Type: multipart/mixed; boundary=0000_032

--0000_032
Content-Type: application/pgp-signature

-----BEGIN PGP SIGNATURE-----
Version: PGP for Personal Privacy 5.0
Comment: Hash computed using SHA-1 micalg (FIPS 180-1).

iQCVAwUBM0It9qHBOF9KrwDlAQFBaQQAisIzQUgyknT2v729b7MImcUc3ROdRBh6
nwMyAfdewQYCDxqdDWvnD1UWoUjwjA1JNA6qhTXBxs8yPtZdDZaguOG2zWawyat9
Jib556AuSx10psREDC3vNsaJ99MV8SKFF92H53l9w/YhVOA0aMZeNfLE0jJVypkY
/so4/7DHhqQ=
=/wlj
```

```
-----END PGP SIGNATURE-----

--0000_032
Content-Type: application/x-pkcs7-signature
Content-Transfer-Encoding: base64
Comment: Hash computed using S/MIME MD5 micalg.

MIAGCSqGSIb3DQEHAqCAMIACAQExDjAMBggqhkiG9w0CBQUAMIAGCSqGSIb3DQEH


[signature material removed]
```



```
+kNIWIbxNiNje1wlzIhaGjrGrOnvYc8+tFn2LgAAAAAAAAAA

--0000_032
Content-Type: application/pgp-signature

-----BEGIN PGP SIGNATURE-----
Version: PGP 2.6.2
Comment: Hash computed using MD5 micalg.

iQCVAwUBM0Iu16HBOF9KrwDlAQGaiQP9EU1YXgMSoNxDAqSmo7UoCE52DuYCfxm7
x8RfRr9+Xz3nPFytSYM2TIWGMeKi1fVr5PhfjdrKvOh9sCq97h6zndZVpGA9x62k
mPVn/QY3fz1eOdyJbYvW4ba7WQll5OoA6cqmEb9tWwh4ra4yE8hZMnLS9a0uPpuB
5dpiTTAE/gY=
=hD3D
-----END PGP SIGNATURE-----

--0000_032--

--0000_031--
```

3. Security Considerations

Use of this protocol has the same security considerations as RFC 1847 and the individual digital signature protocols used. It is not known to either increase or decrease the security of messages using it.

Users should be aware of the fact that each individual signature can be broken out and used to create a valid "multipart/signed" body according to the underlying protocol and RFC 1847.

4. Acknowledgements

We thank Jim Galvin, Sandy Murphy, Steve Crocker, and Ned Freed for their pioneering work on security using MIME multiparts, on which the refinement specified in this document is based.

This draft document relies on the work of the IETF's OpenPGP Working Group.

5. Addresses of the Authors and OpenPGP Working Group Chair

The OpenPGP working group can be contacted via the current chair:

John W. Noerenberg, II
Qualcomm, Inc.
5775 Morehouse Dr.
San Diego, CA 92121 USA
Email: jwn2@qualcomm.com

The principal authors of this draft are:

Dave Del Torto
CryptoRights Foundation
80 Alviso Street, Mailstop: CRF
San Francisco, CA 94127 USA
Tel: +1 415 334 5533
Email: ddt@cryptorights.org, ddt@openpgp.net

Raph Levien
University of California at Berkeley
579 Soda Hall
Berkeley, CA 94720 USA
Tel: +1 510 642 6509
Email: raph@acm.org

Thomas Roessler
Nordstrasse 99
D-53111 Bonn
Germany
Tel.: +49 228 638007
Email: roessler@does-not-exist.org

References

[1] Galvin, J., Murphy, G., Crocker, S., and N. Freed, "Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted", RFC 1847, October 1995.

[2] Galvin, J., Murphy, G., Crocker, S., and N. Freed, "MIME Object Security Services", RFC 1848, October 1995.

[3] Callas, J., Donnerhacke, L., Finney, H., Thayer, R., "OpenPGP Message Format", RFC 2440, November 1998.

[4] Elkins, M., "MIME Security with Pretty Good Privacy (PGP)", RFC 2015, October 1996.

Full Copyright Notice

HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.