openpgp
Internet-Draft
Updates: 3156 (if approved)
Intended status: Informational
Expires: 9 February 2026

A. Gallagher
PGPKeys.EU

8 August 2025

Media Types for OpenPGP
draft-gallagher-openpgp-media-types-00

Abstract

This document updates the specification of existing media types, and specifies additional media types, for the identification of OpenPGP data in non-MIME contexts.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://andrewgdotcom.gitlab.io/openpgp-media-types. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-gallagher-openpgp-media-types/.

Discussion of this document takes place on the OpenPGP Working Group mailing list (mailto:openpgp@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/openpgp/. Subscribe at https://www.ietf.org/mailman/listinfo/openpgp/.

Source for this draft and an issue tracker can be found at https://gitlab.com/andrewgdotcom/openpgp-media-types.

Status of This Memo

This Internet-Draft will expire on 9 February 2026.

Table of Contents

1. Introduction

[RFC3156] specifies media types for use in multipart MIME messages ([RFC1847]), but these are not sufficient for use in other contexts, such as web-based APIs. Valid OpenPGP data formats that are not supported by the currently-specified media types include:

* non-ASCII-armored data

* non-MIME signed or encrypted messages

* Transferable Secret Keys

We wish to define media types to cover all valid OpenPGP data formats, so that they can be accurately represented in applications that rely on media types for content identification, such as web-based APIs.

2. Conventions and Definitions

The term "OpenPGP Certificate" is used in this document interchangeably with "OpenPGP Transferable Public Key", as defined in Section 10.1 of [RFC9580].

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Existing Media Types

[RFC3156] specifies the following media types:

Type	Extension	Description
application/ pgp-encrypted	(none)	The "control part" of a multipart/ encrypted OpenPGP message
application/ pgp-signature	asc, sig.	An ASCII-armored OpenPGP signature packet
application/ pgp-keys	asc	An ASCII-armored sequence of one or more OpenPGP Transferable Public Keys

Table 1: Existing OpenPGP Media Types

The application/pgp-encrypted media type does not directly represent an OpenPGP data format, but the plaintext "control part" of an enclosing multipart/encrypted MIME part -- the encrypted message part uses the application/octet-stream media type instead. It is therefore of little use outside the confines of a multipart/encrypted MIME part.

The other two media types identify ASCII-armored OpenPGP data formats, and are in general use. For example, many keyservers serve OpenPGP certificates using an HTTP response with the content type application/pgp-keys.

3.1. Updates to Existing Media Types

It is established (but currently unspecified) practice for web APIs to serve v4 detached revocation signatures (Section 10.1.3 of [RFC9580]) in the same packet sequence as OpenPGP certificates, e.g. in [I-D.gallagher-openpgp-hkp] and [I-D.koch-openpgp-webkey-service].

The specification of application/pgp-keys is hereby extended to allow zero or more v4 detached revocations to precede any certificates in the OpenPGP packet sequence.

4. New Media Types

The following media types are hereby specified:

Type	Extension	Description
application/pgp-secret-keys	asc	An ASCII-armored sequence of one or more OpenPGP Transferable Secret Keys
application/pgp-message	asc	An ASCII-armored OpenPGP message (Section 6.2 of [RFC9580])

Table 2: New OpenPGP Media Types

As these are all ASCII-armored formats by default, they share the .asc file extension.

5. New Media Type Parameters

OpenPGP does not require the use of ASCII armor. Encoding and decoding ASCII armor in binary-safe contexts (such as HTTP) is therefore wasteful.

To accurately indicate the use of OpenPGP’s native binary wire format, we specify optional parameters (Section 5 of [RFC2045]) for all the OpenPGP media types, with the exception of application/pgp-encrypted. OpenPGP media type parameters MUST NOT be used with the application/pgp-encrypted media type.

Parameter	Optional	Default value	Description
armor	yes	true	Whether the OpenPGP packet sequence is ASCII-armored

Table 3: OpenPGP Media Type Parameters

The armor parameter has the following allowed values:

Value	Extension	Description
true	asc, sig	An armored OpenPGP packet sequence
false	pgp	An un-armored OpenPGP packet sequence

Table 4: OpenPGP Armor Parameter Values

For OpenPGP media types, armor=false indicates that ASCII armor has NOT been applied to the binary wire format. The .asc and .pgp file extensions correspond the value of the armor parameter, but are otherwise shared between the various OpenPGP media types.

To ensure backwards compatibility with existing implementations:

* the absence of an armor parameter implies armor=true.

* the exceptional use of the sig extension for an ASCII-armored detached signature is retained.

6. Guidance for the Future Specification of Media Type Suffixes

No media type suffixes are currently specified for any OpenPGP media type, however future documents may do so. For example, one such document could specify an application/pgp-keys+json format where the packet sequence has been parsed into an abstract syntax tree that is then represented by JSON object structure. (This is not a purely theoretical question, as such a JSON format is already implemented by some applications, for example the [Hockeypuck] keyserver.)

Any suffixed media type uses the data encoding specified for the suffix. The armor parameter MUST NOT be used in combination with any suffixed OpenPGP media type, since ASCII-armor is only specified in relation to the native OpenPGP wire format.

7. Guidance for Implementers

It is RECOMMENDED that new applications in binary-safe contexts, such as web APIs, use armor=false.

ASCII-armor SHOULD continue to be used in 7-bit contexts, such as email. An explicit armor=true parameter SHOULD NOT be added to existing applications, to preserve backwards compatibility, but SHOULD be used in new applications.

8. Security Considerations

The first octet of un-armored OpenPGP data always has the high bit set, therefore the 7-bit clean text of ASCII armor cannot be misinterpreted as the start of an un-armored OpenPGP packet sequence. The armor parameter is therefore highly indicative but not essential for correct parsing of an OpenPGP packet sequence.

9. IANA Considerations

IANA is requested to register the following new templates in the "Media Types" registry, where ((THIS DOCUMENT)) should be replaced by the RFC number of this document:

* application/pgp-secret-keys:

MIME media type name: application
MIME subtype name: pgp-secret-keys
Required parameters: none
Optional parameters: armor

Encoding considerations:

The content of this media type consists of 7bit text if the ‘armor‘ parameter does not have the value ‘false‘.

Security considerations:

See RFC 9580 Section 13.

Interoperability considerations: none

Published specification:

RFC9580 and ((THIS DOCUMENT)).

Additional information:

Magic number(s): none
File extension(s): asc, pgp
Macintosh File Type Code(s): none

Person & email address to contact for further information:

Andrew Gallagher
Email: andrewg&andrewg.com

Intended usage: common

Author/Change controller:

Andrew Gallagher
Email: andrewg&andrewg.com

* application/pgp-message:

MIME media type name: application
MIME subtype name: pgp-message
Required parameters: none
Optional parameters: armor

Encoding considerations:

The content of this media type consists of 7bit text if the ‘armor‘ parameter does not have the value ‘false‘.

Security considerations:

See RFC 9580 Section 13.

Interoperability considerations: none

Published specification:

RFC 9580 and ((THIS DOCUMENT)).

Additional information:

Magic number(s): none
File extension(s): asc, pgp
Macintosh File Type Code(s): none

Person & email address to contact for further information:

Andrew Gallagher
Email: andrewg&andrewg.com

Intended usage: common

Author/Change controller:

Andrew Gallagher
Email: andrewg&andrewg.com

IANA is also requested to update the following existing templates in the "Media Types" registry, where ((THIS DOCUMENT)) should be replaced by the RFC number of this document:

* application/pgp-signature:

MIME media type name: application
MIME subtype name: pgp-signature
Required parameters: none
Optional parameters: armor

Encoding considerations:

The content of this media type consists of 7bit text if the ‘armor‘ parameter does not have the value ‘false‘.

Security considerations:

See RFC 9580 Section 13.

Interoperability considerations: none

Published specification:

RFC9580, RFC 3156, and ((THIS DOCUMENT)).

Additional information:

Magic number(s): none
File extension(s): asc, sig, pgp
Macintosh File Type Code(s): pgDS

Person & email address to contact for further information:

Andrew Gallagher
Email: andrewg&andrewg.com

Intended usage: common

Author/Change controller:

Andrew Gallagher
Email: andrewg&andrewg.com

* application/pgp-keys:

MIME media type name: application
MIME subtype name: pgp-keys
Required parameters: none
Optional parameters: armor

Encoding considerations:

The content of this media type consists of 7bit text if the ‘armor‘ parameter does not have the value ‘false‘.

Security considerations:

See RFC 9580 Section 13.

Interoperability considerations: none

Published specification:

RFC 9580, RFC 3156, and ((THIS DOCUMENT)).

Additional information:

Magic number(s): none
File extension(s): asc, pgp
Macintosh File Type Code(s): none

Person & email address to contact for further information:

Andrew Gallagher
Email: andrewg&andrewg.com

Intended usage: common

Author/Change controller:

Andrew Gallagher
Email: andrewg&andrewg.com

10. References

10.1. Normative References

[RFC2045] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, DOI 10.17487/RFC2045, November 1996, <https://www.rfc-editor.org/rfc/rfc2045>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC3156] Elkins, M., Del Torto, D., Levien, R., and T. Roessler, "MIME Security with OpenPGP", RFC 3156, DOI 10.17487/RFC3156, August 2001, <https://www.rfc-editor.org/rfc/rfc3156>.

[RFC6838] Freed, N., Klensin, J., and T. Hansen, "Media Type Specifications and Registration Procedures", BCP 13, RFC 6838, DOI 10.17487/RFC6838, January 2013, <https://www.rfc-editor.org/rfc/rfc6838>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC9580] Wouters, P., Ed., Huigens, D., Winter, J., and Y. Niibe, "OpenPGP", RFC 9580, DOI 10.17487/RFC9580, July 2024, <https://www.rfc-editor.org/rfc/rfc9580>.

10.2. Informative References

[Hockeypuck] "Hockeypuck OpenPGP Keyserver", n.d., <https://hockeypuck.io>.

[I-D.gallagher-openpgp-hkp] Shaw, D. and A. Gallagher, "OpenPGP HTTP Keyserver Protocol", Work in Progress, Internet-Draft, draft-gallagher-openpgp-hkp-07, 18 March 2025, <https://datatracker.ietf.org/doc/html/draft-gallagher-openpgp-hkp-07>.

[I-D.koch-openpgp-webkey-service] Koch, W., "OpenPGP Web Key Directory", Work in Progress, Internet-Draft, draft-koch-openpgp-webkey-service-20, 2 June 2025, <https://datatracker.ietf.org/doc/html/draft-koch-openpgp-webkey-service-20>.

[RFC1847] Galvin, J., Murphy, S., Crocker, S., and N. Freed, "Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted", RFC 1847, DOI 10.17487/RFC1847, October 1995, <https://www.rfc-editor.org/rfc/rfc1847>.

Appendix A. Acknowledgments

The author would like to thank Daniel Huigens, Daniel Kahn Gillmor, Heiko Sch辰fer and Wiktor Kwapisiewicz for suggestions and discussions.

Author’s Address

Andrew Gallagher
PGPKeys.EU
Email: andrewg@andrewg.com