openpgp
Internet-Draft
Updates: 9580 (if approved)
Intended status: Standards Track
Expires: 7 May 2026

A. Gallagher, Ed.
PGPKeys.EU

3 November 2025

User Attributes in OpenPGP
draft-gallagher-openpgp-user-attributes-01

Abstract

This document updates the specification of User Attribute Packets and Subpackets in OpenPGP.

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-user-attributes. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-gallagher-openpgp-user-attributes/.

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-user-attributes.

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 https://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 7 May 2026.

Table of Contents

1. Introduction

User Attributes are a much-maligned and often-abused feature of OpenPGP. Currently their only specified use is to contain images, however it is known that some implementations use the Private and Experimental User Attribute Subpacket range for various internal purposes.

In this document, we simplify the specification of User Attribute packets and subpackets, and use them to implement currently-missing functionality in OpenPGP.

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 term "Component key" is used in this document to mean either a primary key or subkey.

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. User Attribute Subpackets

User Attribute Packets are simple containers for one or more User Attribute Subpackets. These subpackets are wire-format compatible with Signature Subpackets, but the only currently defined type is the Image Attribute Subpacket type.

3.1. Image Attribute Subpacket

The Image Attribute Subpacket (Type 1) has some unusual features, and is over-specified:

* The image header has a little-endian length field, uniquely for OpenPGP.

* It has a version octet that represents an entire registry but with only one version specified.

* It has an encoding format octet that represents an entire registry with only one value specified.

* The v1 image header has a further 12 octets of unused fields.

The Image Attribute Subpacket has been abused to store large amounts of data on the OpenPGP keyservers, and as a result most modern keyservers refuse to handle any User Attribute packets. Further, we wish to minimise the quantity of human-readable information in the OpenPGP wire format. Images and other data without meaning at the OpenPGP layer SHOULD instead be stored at the application layer, for example in a vCard [RFC6350].

The use of Image Attribute subpackets is therefore deprecated:

* Code point 1 in the User Attribute Subpacket Registry should be updated to "Image Attribute Subpacket (deprecated)".

* No further Image Attribute versions or encoding formats will be supported; the values of both these fields are hereby fixed at 1.

* The OpenPGP Image Attribute Versions and OpenPGP Image Attribute Encoding Formats registries should be deleted.

A User Attribute packet SHOULD NOT contain more than one Image Attribute subpacket.

3.2. Embedded Signature Attribute Subpacket

The Embedded Signature attribute subpacket (Type 2) is analogous to the Embedded Signature signature subpacket (Section 5.2.3.34 of [RFC9580]). It contains a single, complete Signature packet body.

A User Attribute Packet MAY contain one or more Embedded Signature attribute subpackets. These can be used to distribute signatures that cannot otherwise be included in the certificate packet grammar.

Placing embedded signatures in User Attribute subpackets rather than signature subpackets avoids several issues arising from signature cumulation rules. For example, if an embedded signature is included in the hashed or unhashed subpackets area of another signature, it must be duplicated into all future signatures over the same subject. Otherwise, a receiving implementation that ignores or discards older signature packets might ignore or discard the embedded signature.

Unless otherwise specified, all signatures embedded in User Attribute packets MUST be made by a component key of the current certificate.

We update the following signature types to be "embeddable" (see Section 5 of [I-D.gallagher-openpgp-signatures]), and specify their use in User Attributes:

3.2.1. Certification Revocation Signature

An Embedded Signature attribute subpacket MAY contain a Certification Revocation signature (Type 0x30):

3.2.1.1. Certification Revocation Signature Over a Third-Party Certificate

The key holder might not trust that a third party will distribute certification revocations over their (possibly fraudulent) certificate. The key holder MAY instead distribute the revocation signature in their own certificate using an Embedded Signature attribute subpacket of a User Attribute packet. A receiving implementation SHOULD apply any certification revocation to the target certification, if the revocation signature correctly validates.

To aid a receiving implementation locate the correct certificate to apply the revocation to, a generating implementation SHOULD include an Intended Recipient Fingerprint subpacket Section 5.2.3 of [RFC9580] containing the fingerprint of the primary key over which the revocation has been calculated. The receiving implementation then only has to perform one signature verification per User ID packet on the target certificate, but cannot recover the contents of a User ID packet that it does not already have a copy of.

3.2.1.2. Certification Revocation Self-Signature

If the key holder wishes to delete a User ID or User Attribute from their own certificate using a redacting revocation signature (Section 5.1 of [I-D.dkg-openpgp-abuse-resistant-keystore]), they cannot append the revocation signature to the redacted User ID or User Attribute packet, because the redacted packet is no longer part of the certificate packet sequence. In order to distribute the revocation signature, it MAY be included in an Embedded Signature attribute subpacket of a separate User Attribute packet. The revocation signature can be validated by a receiving implementation that already has a copy of the redacted User ID or User Attribute.

3.3. User Attribute Subpacket Grammar

A User Attribute MUST NOT contain subpackets of more than one type. A receiving implementation MUST disregard the entire User Attribute packet if it contains subpackets of more than one type.

A certification signature over a User Attribute packet SHOULD NOT contain subpackets of the Direct or First Party Certification categories (Section 7.2 of [I-D.gallagher-openpgp-signatures]), and any such subpackets MUST be ignored.

4. Security Considerations

The deprecation of Image Attribute subpackets should increase both security and reliability, by removing a significant abuse vector.

Distribution of third-party revocations in the certificate of the signer should be more reliable than existing methods, thereby increasing overall trust in the certification process.

5. IANA Considerations

IANA is requested to perform the following tasks:

* Delete the OpenPGP Image Attribute Versions and OpenPGP Image Attribute Encoding Format registries.

* Update the contents of the OpenPGP User Attribute Subpacket Types Registry to read:

Type	Name	Reference
1	Image Attribute (Deprecated)	Section 3.1
2	Embedded Signature	Section 3.2

Table 1: OpenPGP User Attribute Subpacket Types

* Update the following entry in the OpenPGP Signature Types Registry to read:

ID	Name	Embeddable	Reference
0x30	Certification Revocation Signature	Yes	[RFC9580], Section 3.2.1

Table 2: OpenPGP Signature Types (update)

6. References

6.1. Normative References

[I-D.dkg-openpgp-revocation]
Gillmor, D. K. and A. Gallagher, "Revocation in OpenPGP", Work in Progress, Internet-Draft, draft-dkg-openpgp-

revocation-02, 28 March 2025,
<https://datatracker.ietf.org/doc/html/draft-dkg-openpgp-revocation-02>.

[I-D.gallagher-openpgp-signatures]
Gallagher, A. and D. K. Gillmor, "OpenPGP Signatures and Signed Messages", Work in Progress, Internet-Draft, draft-gallagher-openpgp-signatures-02, 3 November 2025, <https://datatracker.ietf.org/doc/html/draft-gallagher-openpgp-signatures-02>.

[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>.

[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>.

6.2. Informative References

[I-D.dkg-openpgp-abuse-resistant-keystore]
Gillmor, D. K., "Abuse-Resistant OpenPGP Keystores", Work in Progress, Internet-Draft, draft-dkg-openpgp-abuse-resistant-keystore-06, 18 August 2023, <https://datatracker.ietf.org/doc/html/draft-dkg-openpgp-abuse-resistant-keystore-06>.

[RFC6350] Perreault, S., "vCard Format Specification", RFC 6350, DOI 10.17487/RFC6350, August 2011, <https://www.rfc-editor.org/rfc/rfc6350>.

Appendix A. Acknowledgments

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

Appendix B. Document History

Note to RFC Editor: this section should be removed before publication.

B.1. Changes Between draft-gallagher-openpgp-attributes-00 and draft-gallagher-openpgp-attributes-01

* Removed Attribute Creation Time, Attribute URI, and Notation Data subpacket types.
* Restricted Signature Subpacket categories in certifications over User Attributes.
* Simplified the User Attribute Subpacket grammar and registry requirements.
* Specified use of the Intended Recipient Fingerprint subpacket.
* Added references.

Author’s Address

Andrew Gallagher (editor)
PGPKeys.EU
Email: andrewg@andrewg.com