

openpgp  
Internet-Draft  
Updates: 9580 (if approved)  
Intended status: Standards Track  
Expires: 15 August 2025

A. Gallagher, Ed.  
PGPKeys.EU  
11 February 2025

User Attributes in OpenPGP  
draft-gallagher-openpgp-user-attributes-00

## 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 15 August 2025.

## Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

## Table of Contents

1. Introduction . . . . .	3
2. Conventions and Definitions . . . . .	3
3. User Attribute Subpackets . . . . .	3
3.1. User Attribute Subpacket Categories . . . . .	3
3.1.1. General Subpackets . . . . .	3
3.1.2. Attribute Value Subpackets . . . . .	4
3.2. Image Attribute Subpacket . . . . .	4
3.3. Attribute Creation Time Subpacket . . . . .	5
3.4. Attribute URI Subpacket . . . . .	5
3.5. Notation Data Subpacket . . . . .	6
3.6. Embedded Signature Subpacket . . . . .	6
3.6.1. Certification Revocation Signature . . . . .	6
4. User Attribute Subpacket Grammar . . . . .	7
5. Time Evolution of User Attributes . . . . .	7
6. Security Considerations . . . . .	8
7. IANA Considerations . . . . .	9
7.1. Guidelines for Management of the User Attribute Subpacket Types Registry . . . . .	10
8. References . . . . .	10
8.1. Normative References . . . . .	10
8.2. Informative References . . . . .	10
Appendix A. Acknowledgments . . . . .	11
Author's Address . . . . .	11

## 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. As a result, a User Attribute Packet is currently only used to contain an Image Attribute Subpacket.

### 3.1. User Attribute Subpacket Categories

By analogy with the categorisation of Signature Subpacket Types in Section 7 of [I-D.gallagher-openpgp-signatures], we categorise User Attribute Subpacket Types into:

#### 3.1.1. General Subpackets

These may be included in any User Attribute packet, and define properties of the packet itself. Unless otherwise specified, a User Attribute Packet SHOULD NOT contain more than one of each type of General subpacket.

### 3.1.2. Attribute Value Subpackets

These carry the non-metadata content of the User Attribute. Unless otherwise specified, a User Attribute Packet SHOULD NOT contain more than one Attribute Value subpacket. A User Attribute Packet MUST NOT contain subpackets of more than one type of Attribute Value subpacket.

### 3.2. Image Attribute Subpacket

The Image Attribute Subpacket (Type 1, Attribute Value category) has some unusual features, and is wildly 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 key servers, and as a result most modern key servers refuse to handle any User Attribute packets. Further, we wish to minimise the quantity of human-readable information in the OpenPGP wire format. If a key owner wishes to publish an image, this is more appropriately handled at the application layer.

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)", with a category of "Attribute Value".
- \* 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 MUST NOT contain more than one Image Attribute subpacket.

### 3.3. Attribute Creation Time Subpacket

We define an Attribute Creation Time subpacket (Type 2, General category) that identifies the time before which the User Attribute packet is not valid. It contains a four-octet timestamp in seconds since midnight, 1st January 1970. It is bitwise-identical to the Signature Creation Time Signature Subpacket (Section 5.2.3.11 of [RFC9580]), and performs the same function as the "creation time" field in a Public Key or Public Subkey packet (Section 5.5.2 of [RFC9580]).

A User Attribute packet MUST NOT contain more than one Attribute Creation Time subpacket.

### 3.4. Attribute URI Subpacket

We define an Attribute URI Subpacket (Type 8 (TBC), Attribute Value category) that identifies the resource being claimed by the key owner. It performs a similar function to the User ID packet, but in a strictly machine-readable URI format. For example, an email address would be represented as "mailto:user@example.com".

A certificate MAY include both a User ID containing an email address, and a User Attribute with an Attribute URI subpacket representing the same email address. If a receiving implementation supports the Attribute URI subpacket, it SHOULD be used in preference to the User ID packet.

If an implementation intends to certify the email address component of an RFC822-ish User ID, but not the real name or comment components, it SHOULD instead certify a User Attribute with an Attribute URI subpacket containing the mailto: URI of the email address.

Section 10.1 of [RFC9580] indicates that a User ID packet is not necessary in a v4 or v6 certificate (this differs from previous versions of the OpenPGP specification). However, since legacy implementations will not in general understand the Attribute URI subpacket, it is RECOMMENDED that a v4 certificate includes a User ID packet corresponding to each Attribute URI subpacket.

A User Attribute packet MUST NOT contain more than one Attribute URI subpacket.

### 3.5. Notation Data Subpacket

The Notation Data Subpacket (Type 20, General category) from the Signature Subpacket Types registry is duplicated into the User Attribute Subpacket registry, with the same wire format (Section 5.2.3.24 of [RFC9580]).

A User Attribute Packet MAY contain one or more Notation Data subpackets. Notation names share the same namespaces and semantics as signature notations. Notation names in the user namespace MAY be present in User Attributes. Notation names in the IANA namespace MUST NOT be present in User Attributes unless specified for that purpose.

### 3.6. Embedded Signature Subpacket

The Embedded Signature Subpacket (Type 32, Attribute Value category) from the Signature Subpacket Types registry is duplicated into the User Attribute Subpacket registry, with the same wire format (Section 5.2.3.34 of [RFC9580]).

A User Attribute Packet MAY contain one or more Embedded Signature subpackets. These can be used by an implementation that wishes to distribute signatures that would not otherwise be valid in a certificate. Unless otherwise specified, all such embedded signature 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:

#### 3.6.1. Certification Revocation Signature

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

##### 3.6.1.1. 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 [REVOC-16]. The key holder MAY instead distribute the revocation signature in their own certificate using an Embedded Signature subpacket of a User Attribute packet.

(( TODO: can we identify the third party certificate in the revocation sig? ))

### 3.6.1.2. 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 [REVOC-2], 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 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.

## 4. User Attribute Subpacket Grammar

- \* A User Attribute packet SHOULD contain exactly one Attribute Creation Time subpacket.
- \* It SHOULD contain at most one subpacket of each other subpacket type in the General category.
- \* It MUST NOT contain subpackets of more than one type in the Attribute Value category.

A receiving implementation MUST disregard the entire User Attribute packet if a User Attribute packet contains an unknown subpacket, or if it contains subpackets of more than one type in the Attribute Value category.

## 5. Time Evolution of User Attributes

There has historically been no easy way to create a Certification signature at an arbitrary time that supersedes an earlier one but retains the same starting validity date. Therefore, many implementations maintain a copy of all Certification signatures to ensure that historical signatures can be validated after a superseding certification is made. Some implementations have also attempted to work around this by backdating signature creation timestamps, which has implications for signature ordering.

We are prevented from using the time evolution semantics described in Section 8.2 of [I-D.gallagher-openpgp-signatures] for Certification signatures over User IDs, because User IDs have no intrinsic creation date. It is instead RECOMMENDED that v6 (and higher) certificates use User Attributes that contain an Attribute Creation Time subpacket.

Certification signatures over a User Attribute with an Attribute Creation Time subpacket ({attribute-creation-time-subpacket}) can therefore have similar time evolution semantics as binding signatures, with the Attribute Creation Time subpacket performing the role of the (Sub)key Creation Time field.

1. Certification signatures SHOULD NOT contain Key Expiration Time subpackets, and any such subpackets MUST be ignored.
2. The validity of a Certification signature over a User Attribute extends from the User Attribute Creation Time until the signature's expiration time.
3. If the most recent Certification signature has no Signature Expiration Time subpacket, then the certification does not expire.
4. A Certification signature is temporally valid if its creation time is no earlier than the creation times of all of the primary key that made it, and the primary key and User Attribute that it is made over.
5. Unlike a Key Binding self-signature, a Certification self-signature is not valid if the primary key has been hard-revoked, even for historical purposes.
6. The creation time of a Certification signature over a User Attribute is used only for ordering, not for calculation of User Attribute validity.

A third-party Certification signature over a User Attribute thereby retrospectively validates the User Attribute from the User Attribute Creation Time, if it exists. If a user does not believe that such a User Attribute has always been valid, they should not certify it.

## 6. Security Considerations

The use of an Attribute URI subpacket instead of a User ID packet should increase overall security, as it has a stricter format that simplifies parsing.

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.



## 7. IANA Considerations

IANA is requested to perform the following tasks:

- \* Delete the OpenPGP Image Attribute Versions and OpenPGP Image Attribute Encoding Format registries.
- \* Add a column to the OpenPGP User Attribute Subpacket Types Registry, called "Category".
- \* Update the contents of the OpenPGP User Attribute Subpacket Types Registry to read:

Type	Name	Category	Reference
1	Image Attribute (Deprecated)	Attr Value	Section 3.2
2	Attribute Creation Time	General	Section 3.3
8(TBC)	Attribute URI	Attr Value	Section 3.4
20	Notation Data	General	Section 3.5
32	Embedded Signature	Attr Value	Section 3.6

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	Yes	[RFC9580],
	Revocation Signature		Section 3.6.1

Table 2: OpenPGP Signature Types (update)

### 7.1. Guidelines for Management of the User Attribute Subpacket Types Registry

We have allocated code points in the User Attribute Subpacket Types registry that permit wire-format and semantics compatibility between User Attribute subpackets and Signature subpackets. Code points 1 and 8 are reserved in the Signature Subpacket Types registry, and code points 2, 10 and 32 represent subpacket types that are compatible in wire format and semantics. While not strictly required, it is RECOMMENDED that code points should be allocated so as to minimise semantics and wire format incompatibility between the two Subpacket Type registries. Signature subpacket code points outside of the General or Attribute Value categories SHOULD NOT be shared with the User Attribute registry.

## 8. References

### 8.1. Normative References

- [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>>.

### 8.2. Informative References

- [I-D.dkg-openpgp-revocation] Gillmor, D. K., "Revocation in OpenPGP", Work in Progress, Internet-Draft, draft-dkg-openpgp-revocation-01, 17 August 2023, <<https://datatracker.ietf.org/doc/html/draft-dkg-openpgp-revocation-01>>.
- [I-D.gallagher-openpgp-signatures] Gallagher, A., "OpenPGP Signatures and Signed Messages", Work in Progress, Internet-Draft, draft-gallagher-openpgp-signatures-00, 7 November 2024, <<https://datatracker.ietf.org/doc/html/draft-gallagher-openpgp-signatures-00>>.

[REVOC-16] Gallagher, A., "Distribution of revocations", 14 April 2024, <<https://gitlab.com/dkg/openpgp-revocation/-/issues/16>>.

[REVOC-2] Gallagher, A., "RTBF self-sovereignty via revocations", 5 March 2024, <<https://gitlab.com/dkg/openpgp-revocation/-/issues/2>>.

#### Appendix A. Acknowledgments

The author would like to thank Heiko Sch<sub>辰</sub>fer for discussions.

#### Author's Address

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