openpgp
Internet-Draft
Updates: 9580 (if approved)
Intended status: Standards Track
Expires: 9 February 2026

A. Gallagher, Ed.
PGPKeys.EU

8 August 2025

GREASE Code Points in OpenPGP
draft-gallagher-openpgp-grease-01

Abstract

This document reserves code points in various OpenPGP registries for use in interoperability testing, by analogy with GREASE in TLS.

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

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-grease.

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 9 February 2026.

Table of Contents

1. Introduction

GREASE [RFC8701] is an existing specification to ensure forwards compatibility of assigned code points in TLS. We wish to specify a similar mechanism for OpenPGP. This will be particularly useful in the OpenPGP Interoperability Test Suite [INTEROP], but is not restricted to controlled environments. It is expected that implementations will include PGP-GREASE code points in real-world artifacts on an ongoing basis, to encourage forwards-compatible coding across multiple implementations.

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].

For avoidance of confusion with GREASE in TLS, we will use the term "PGP-GREASE" for the equivalent mechanism in OpenPGP.

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. Reservation of PGP-GREASE Code Points

We assign the following one-octet code points to PGP-GREASE:

Sequence	Code Point (Decimal)	Code Point (Hexadecimal)
1	51	0x33
2	58	0x3a
3	68	0x44
4	75	0x4b
5	85	0x55
6	92	0x5c
7	119	0x77
8	126	0x7e

Table 1: OpenPGP GREASE Code Points

These code points will be reserved for PGP-GREASE in the following registries:

Registry Name	Notes
OpenPGP String-to-Key (S2K) Types	(1)
OpenPGP User Attribute Subpacket Types	
OpenPGP Image Attribute Encoding Format	
OpenPGP Signature Subpacket Types	(2)
OpenPGP Reason for Revocation (Revocation Octet)	(1)
OpenPGP Public Key Algorithms	
OpenPGP Symmetric Key Algorithms	
OpenPGP Hash Algorithms	
OpenPGP Compression Algorithms	
OpenPGP Secret Key Encryption (S2K Usage Octet)	(3)
OpenPGP Signature Types	
OpenPGP Image Attribute Versions	
OpenPGP AEAD Algorithms	
OpenPGP Key and Signature Versions	

Table 2: OpenPGP GREASE Registries

1. The use of PGP-GREASE code points in the String-to-Key Types and Reason for Revocation registries is not currently specified, however the code points will be reserved for consistency.

2. When PGP-GREASE code points from the Signature Subpacket Types registry are used, the critical bit MUST NOT be set.

3. All code points allocated in the Symmetric Key Algorithms registry are automatically also allocated in the S2K Usage Octet registry.

Due to the smaller number of allocatable code points (63) in the OpenPGP Packet Types registry, and the division of the registry into critical and non-critical ranges, most PGP-GREASE values cannot be

used as Packet Types. In addition, implementations pre-dating [RFC9580] are not required to ignore unknown non-critical packet types. A Marker packet (Section 5.8 of [RFC9580]) SHOULD therefore be used instead. Packet Types 51 and 58 MAY be used if it is known, or it is reasonable to expect, that the receiving implementation supports [RFC9580].

To avoid any potential ambiguity, no PGP-GREASE code points have been assigned in the Private and Experimental range.

Note also that [INTEROP] currently uses signature version 23 as a de-facto GREASE code point.

4. Usage of PGP-GREASE Code Points

An implementation MAY insert dummy packets or subpackets into otherwise valid packet sequences. It MAY also include dummy code points in preference lists. The data section of dummy packets and subpackets SHOULD contain only the ten octets "PGP-GREASE", in UTF-8 encoding. All other fields of dummy packets and subpackets SHOULD correspond to those of a real packet or subpacket.

A generating implementation SHOULD choose code points deterministically, while ensuring that all PGP-GREASE code points are eventually used.

(TODO: how often should we add GREASE?)

A receiving implementation MUST gracefully ignore unknown code points when required to by [RFC9580], including PGP-GREASE code points. It MUST NOT treat PGP-GREASE code points any differently from other unknown code points; this includes detecting or indicating the presence of PGP-GREASE code points.

PGP-GREASE codepoints MAY be used in either certificates or messages.

Since existing legacy implementations have not consistently followed the requirement to ignore unknown code points, a generating implementation is RECOMMENDED to introduce PGP-GREASE code points gradually, over several release cycles. This should ensure that legacy receiving implementations are not overwhelmed by errors in a short period of time.

4.1. Certificates

An implementation MAY use PGP-GREASE codepoints in the following certificate contexts:

* Dummy algorithm IDs in algorithm-preference signature subpackets (subpacket types 11, 21, 22, and 39).

* Signature subpacket IDs of dummy signature subpackets, in either the hashed or unhashed area.

* User attribute subpacket types, versions and encoding formats of dummy user attribute subpackets.

* Packet versions and algorithm IDs in dummy subkey packets.

* Signature and hash algorithm IDs and signature version numbers in dummy third-party certification signatures.

* Hash algorithm IDs in dummy self-signatures.

* Packet and signature types in dummy packets.

A generating implementation MAY also generate dummy primary keys with PGP-GREASE version numbers or algorithm IDs.

4.2. Messages

An implementation MAY use PGP-GREASE codepoints in the following message contexts:

* Signature subpacket IDs of dummy signature subpackets in the hashed or unhashed signature subpacket area.

* Signature and hash algorithm IDs and signature version numbers in dummy document signature packets and their corresponding OPS packets.

* Packet and signature types in dummy packets.

Note that when an OPS packet is present, any PGP-GREASE code points it contains MUST be duplicated in the corresponding signature packet.

5. Private and Experimental Ranges

Unlike PGP-GREASE reservations, code points in the Private and Experimental ranges MAY be treated specially by a receiving implementation. This MAY include emitting an explicit warning that an unknown code point in the Private and Experimental range has been encountered. To simplify the recognition of Private and Experimental code points, each Private and Experimental range in the OpenPGP group of registries will be expanded to cover the code points 96-111, i.e. 0x60-0x6f. Aligning this range to nybble boundaries will allow the

use of a bit mask, and will provide additional Private and Experimental code points for future use.

6. Security Considerations

Legacy implementations that do not properly ignore unknown code points will experience failures; this is intentional. None of these failures should have security consequences in themselves, unless other coding errors are present in the legacy implementation. While this should result in increased security in the long term, exposing such bugs may cause problems in the short term.

Generating implementations are therefore RECOMMENDED to be cautious in deploying PGP-GREASE initially. In particular, implementations SHOULD NOT generate PGP-GREASE code points in production unless they have been tested first in a controlled environment such as the Interoperability Test Suite [INTEROP].

7. IANA Considerations

IANA is requested to allocate the code points listed in Table 1 in each of the registries listed in Table 2, with the description "Reserved (PGP-GREASE)" and a reference pointing to this document.

IANA is also requested to allocate code points 51 and 58 in the "OpenPGP Packet Types" registry, with the description "Reserved (PGP-GREASE)" and a reference pointing to this document.

IANA is also requested to adjust the extent of the Private and Experimental range in each of the registries listed in Table 2, from "100-110" to "96-111".

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

[INTEROP] "OpenPGP Interoperability Test Suite", n.d., <https://tests.sequoia-pgp.org/>.

[RFC8701] Benjamin, D., "Applying Generate Random Extensions And Sustain Extensibility (GREASE) to TLS Extensibility", RFC 8701, DOI 10.17487/RFC8701, January 2020, <https://www.rfc-editor.org/rfc/rfc8701>.

Appendix A. Acknowledgments

The author would like to thank Daniel Huigens for inspiring this work.

Appendix B. Document History

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

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

* Moved code points.

* Expanded private and experimental ranges.

Author’s Address

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