Network Working Group
Internet-Draft
Updates: 9580 (if approved)
Intended status: Standards Track
Expires: 8 May 2026

D. Huigens, Ed.
Proton AG

4 November 2025

Persistent Symmetric Keys in OpenPGP
draft-ietf-openpgp-persistent-symmetric-keys-02

Abstract

This document defines a new packet and algorithm for the OpenPGP standard (RFC 9580) to support persistent symmetric keys, for message encryption using authenticated encryption with additional data (AEAD) and for message authentication using AEAD authentication tags. This enables the use of symmetric cryptography for data storage (and other contexts that do not require asymmetric cryptography), for improved performance, smaller keys, and improved resistance to quantum computing.

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://twisstle.gitlab.io/openpgp-persistent-symmetric-keys/. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-openpgp-persistent-symmetric-keys/.

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/twisstle/openpgp-persistent-symmetric-keys.

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 8 May 2026.

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

The OpenPGP standard [RFC9580] has supported symmetric encryption for data packets using session keys since its inception, as well as symmetric encryption using password-derived keys. This document extends the use of symmetric cryptography by adding support for persistent symmetric keys which can be stored in a transferable secret key, and used to symmetrically encrypt session keys, for long-term storage and archival of messages. This document uses authenticated encryption with associated data (AEAD) as defined by [RFC9580].

The OpenPGP standard also supports the use of digital signatures for authentication and integrity but no similar symmetric mechanism exists in the standard. This document introduces the use of AEAD authentication tags as a symmetric counterpart to digital signatures, for long-term storage and archival of attestations of authenticity and certification.

2. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119]. Any implementation that adheres to the format and methods specified in this document is called a compliant application. Compliant applications are a subset of the broader set of OpenPGP applications described in [RFC9580]. Any [RFC2119] keyword within this document applies to compliant applications only.

3. Motivation

When compared to asymmetric cryptography, symmetric cryptography can provide improved performance and equivalent security with smaller keys. In contexts that do not require asymmetric cryptography, such as secure data storage where the same user encrypts and decrypts data, symmetric cryptography can be used to take advantage of these benefits.

Additionally, asymmetric algorithms included in OpenPGP are vulnerable to attacks that might become possible on quantum computers [Shor]. Symmetric cryptography is also affected by quantum computing but to a lesser extent, which can be countered by using larger keys [Grover]. While the standardization of quantum-secure asymmetric cryptography in OpenPGP is ongoing [PQCinOpenPGP], and will be required to secure communications, there is a large body of existing messages encrypted with classical algorithms. Once persistent symmetric keys are available, these messages can be protected against

future compromises efficiently by symmetrically re-encrypting the session key, and storing the message symmetrically encrypted for long-term storage and archival.

4. Creating and Reusing Packets

For storing persistent symmetric keys, we introduce a new packet (see Section 5), as handling of persistent symmetric key material requires some care. For example, when extracting a Transferable Public Key from a Transferable Secret Key, persistent symmetric keys must be ignored.

For storing session keys encrypted with persistent symmetric keys, while a Symmetric-Key Encrypted Session Key packet exists, its semantics don't match our requirements, as it's intended to encrypt the session key with a user-provided password, and doesn't offer a way to store a reference to a persistent key. Therefore, we reuse the Public-Key Encrypted Session Key packet instead, which does offer the desired semantics.

Similarly, we reuse the Signature packet for "symmetric signatures".

For these use cases, no new packet is required as the handling of these packets requires no special care.

To indicate the type of keys in the new and existing packets, a special persistent symmetric algorithm ID value 0 is registered, which can be used in the place of a public-key algorithm ID.

5. Persistent Symmetric Key Packet

This document defines a new OpenPGP packet, extending table 3 of [RFC9580].

ID	Critical	Packet Type Description	Shorthand
40	No	Persistent Symmetric Key Packet	PSK

Table 1: Persistent Symmetric Key Packet registration

The Persistent Symmetric Key Packet (Type ID 40) has identical fields to the Secret Key Packet (Type ID 5). However, only version 6 of the packet is defined. Earlier versions of the Secret Key Packet format MUST NOT be used with the Persistent Symmetric Key Packet.

The Persistent Symmetric Key Packet MUST NOT be used with asymmetric algorithms, i.e. any of the public key algorithms defined in table 18 of [RFC9580]. It may only be used with the persistent symmetric algorithm defined below, with special algorithm ID value 0.

When storing encrypted symmetric key material in a Persistent Symmetric Key Packet, AEAD encryption (S2K usage octet 253, see section 3.7.2.1 of [RFC9580]) MUST be used, to ensure that the secret key material is bound to the fingerprint. Implementations MUST NOT decrypt symmetric key material in a Persistent Symmetric Key Packet that was encrypted using a different method.

6. Extended Transferable Secret Key Grammar

The Transferable Secret Key grammar defined in section 10.2 of [RFC9580] is extended to allow including Persistent Symmetric Key Packets. Persistent Symmetric Keys may be included together with asymmetric keys in a single sequence of Transferable Secret Keys. However, Persistent Symmetric Keys do not accept subcomponents, such as subkeys, User IDs, or direct-key signatures.

7. Persistent Symmetric Key Algorithm

This document defines one new algorithm for use with OpenPGP, updating table 18 of [RFC9580].

ID	Algorithm	Public Key Format	Secret Key Format	Signature Format	PKESK Format
0	AEAD	sym. algo, AEAD algo, fingerprint seed [Section 7.1]	key material	IV, authentication tag [Section 7.3]	IV, ciphertext [Section 7.2]

Table 2: Persistent Symmetric Key Algorithm registration

This algorithm ID can be used to store symmetric key material in a Persistent Symmetric Key Packet (see Section 5). It can also be used to store a session key encrypted using AEAD in a PKESK packet (see section 5.1 of [RFC9580]). It can also be used to store an AEAD authentication tag in a Signature packet (see section 5.2 of [RFC9580]).

Implementations MUST NOT use the symmetric algorithm ID in Public-Key Packets, Public-Subkey Packets, Secret-Key Packets or Secret-Subkey Packets.

7.1. Algorithm-Specific Fields for Persistent Symmetric Keys

The public key material consists of this series of values:

* A one-octet symmetric algorithm identifier (see section 9.3 of [RFC9580]).

* A one-octet AEAD algorithm (see section 9.6 of [RFC9580]).

* A 32-octet random seed to randomize the key fingerprint.

The secret key material consists of this single value:

* Symmetric key material of the appropriate length for the given symmetric algorithm.

7.2. Algorithm-Specific Fields for Persistent Symmetric Encryption

The encrypted session key consists of this series of values:

* A initialization vector of the size specified by the AEAD mode of the key.

* A symmetric key encryption of the plaintext value described in section 5.1 of [RFC9580], performed using the symmetric-key cipher and AEAD mode of the key, including the authentication tag.

7.3. Algorithm-Specific Fields for Persistent Symmetric Signatures

The signature consists of this series of values:

* A initialization vector of the size specified by the AEAD mode of the key.

* An authentication tag of the size specified by the AEAD mode of the key, created by encrypting the empty value using the symmetric-key cipher and AEAD mode of the key, with as additional data the hash digest described in section 5.2.4 of [RFC9580].

Although not required by AEAD algorithms, to maintain consistency with existing signature algorithms, AEAD authentication tags are produced from appropriately hashed data, as per section 5.2.4 of [RFC9580].

8. Security Considerations

Security considerations are discussed throughout the document where appropriate.

9. IANA Considerations

9.1. Updates to Packet Types

IANA is requested to update the "OpenPGP Packet Types" registry with the entry in Table 1.

9.2. Updates to Public Key Algorithms

IANA is requested to update the "OpenPGP Public Key Algorithms" registry with the entry in Table 2.

10. Acknowledgements

An initial version of this draft was written by Dan Ristea (Proton AG), with guidance from Dr Philipp Jovanovic (University College London) and the editor.

Thanks to feedback and suggestions from Andrew Gallagher, Heiko Sch辰fer, Justus Winter, Falko Strenzke, and Daniel Kahn Gillmor, in no particular order.

11. References

11.1. Normative References

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, DOI 10.17487/RFC2104, February 1997, <https://www.rfc-editor.org/info/rfc2104>.

[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/info/rfc2119>.

[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/info/rfc9580>.

11.2. Informative References

[Grover] Grover, L., "Quantum mechanics helps in searching for a needle in a haystack", 1997, <https://arxiv.org/abs/quant-ph/9706033>.

[PQCinOpenPGP] Kousidis, S., Strenzke, F., and A. Wussler, "Post-Quantum Cryptography in OpenPGP", October 2023, <https://datatracker.ietf.org/doc/html/draft-wussler-openpgp-pqc-03>.

[Shor] Shor, P., "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", October 1997, <http://dx.doi.org/10.1137/S0097539795293172>.

Author's Address

Daniel Huigens (editor)
Proton AG
Route de la Galaise 32
CH-1228 Plan-les-Ouates
Switzerland
Email: d.huigens@protonmail.com