Security Area Advisory Group
Internet-Draft
Updates: 4880 (if approved)
Intended status: Informational
Expires: July 10, 2018

R. Tse
Ribose

January 6, 2018

IANA Registry Updates for OpenPGP
draft-openpgp-iana-registry-updates-00

Abstract

This document describes a number of changes to the OpenPGP (RFC 4880) IANA registries that range from adding notes to the registry to changing registration policies. These changes were motivated by recently proposed extensions to OpenPGP. Existing IANA OpenPGP registry policies are defined by RFC 4880.

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 July 10, 2018.

Copyright Notice

Table of Contents

1. Introduction

This document instructs IANA to make changes to a number of OpenPGP-related IANA registries [RFC4880]. These changes were motivated by recently proposed extensions to OpenPGP.

Modelled after [I-D.ietf-tls-iana-registry-updates], the document performs a similar function in modifying existing IANA registry policies for OpenPGP [RFC4880].

The changes introduced by this document are intended to be comprehensive, proposed after a thorough review of existing registry policy and values. Changes include updating of registry policy, filling in missing values, providing recommendation of registered items and general housekeeping.

The document lists out each OpenPGP registry individually and provides the rationale for changes and the required changes themselves.

Specifically, the following changes are pursued:

- Alignment of registry policies with [RFC8126];
- Consistency of existing OpenPGP registries, for example, some registries have the prefix "PGP" while some others don't;
- Missing values in registries while having been defined in <<RFC4880>;
- Creating a missed registry defined in [RFC4880], namely the "OpenPGP Signature Notation Data Subpacket Flags" registry;
- A number of references in the registries point to documents that detail a certain algorithm, but should refer to a document (and the relevant section if appropriate) that details the implementation requirements of that algorithm within the context of OpenPGP.

2. Terms and Definitions

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].

The key words "*Private Use*", "*Experimental Use*", "*Hierarchical Allocation*", "*First Come First Served*", "*Expert Review*", "*Specification Required*", "*RFC Required*", "*IETF Review*", "*Standards Action*" and "*IESG Approval*" in this document are to be interpreted as described in Section 4 of [RFC8126].

3. Alignment Amongst OpenPGP Registries

3.1. Policy Conventions Given In RFC 8126

The OpenPGP IANA registries and their policies defined in [RFC4880] pre-date [RFC8126] which defined the term "IETF Review" instead of the now-outdated term "IETF Consensus" [RFC2434].

This draft updates policies of the OpenPGP IANA registries to align with the terms specified in [RFC8126].

3.2. Registry Naming

Registry names of IANA OpenPGP registries *SHOULD* be consistent.

The following registries originally have the "PGP" prefix, and the prefix *SHOULD* be changed to "OpenPGP":

- PGP String-to-Key (S2K) Registry (Section 5.1)
- PGP Packet Types/Tags Registry (Section 5.2)
- PGP User Attribute Types Registry (Section 5.3)

The prefix "OpenPGP" *SHOULD* be added to the following registries:

- Image Format Subpacket Types Registry (Section 5.4)
- Signature Subpacket Types Registry (Section 5.5)
- Signature Notation Data Subpacket Notation Types Registry (Section 5.5)
- Key Server Preference Extensions Registry (Section 5.7)

- Reason for Revocation Extensions Registry (Section 5.8)
- Implementation Features Registry (Section 5.9)
- New Packet Versions Registry (Section 5.10)
- Public Key Algorithms Registry (Section 5.12)
- Symmetric Key Algorithms Registry (Section 5.13)
- Hash Algorithms Registry (Section 5.14)
- Compression Algorithms Registry (Section 5.15)

This renaming is not necessary for the "OpenPGP Signature Notation Data Subpacket Notation Flags Registry" (Section 5.16) since it is newly created according to this convention.

For specific recommendations, please see the corresponding sections in Section 5.

4. Providing Recommendations Via The "Recommended" Column

The feature set of OpenPGP is an evolving one. In some cases, it has been unclear whether implementation of a certain feature would actually be beneficial for interoperability or create fragmentation of implementations.

Moreover, the fast-moving nature of cryptography directly impacts the security of OpenPGP implementations, and an algorithm once considered secure may be subject to cryptanalytic results that advise otherwise. For example, this has been demonstrated by the widespread obsolescence of SHA-1 [SHA1-Coll] [RFC6194].

It is therefore beneficial for all OpenPGP interested parties that implementers can follow a stable reference on what is considered best practice in OpenPGP implementations.

There are two types of recommendations considered here:

- Recommended for security (abbreviated as "REC-S" in this document)
- Recommended for interoperability (abbreviated as "REC-I" in this document)

4.1. Security Recommendations

Recommendations for security are usually critical and urgent.

The following registries shall have the "Security Recommendation" column added:

- PGP String-to-Key (S2K) Registry
- Public Key Algorithms Registry
- Symmetric Key Algorithms Registry
- Hash Algorithms Registry

The allowed values for this column are:

- Yes: Recommended, this algorithm is considered secure;
- No: Not recommended, this algorithm is considered insecure;
- Empty: No comment, there is no recommendation on this algorithm.

A "Security Recommendation" *MUST* only be accepted through an Expert Review described in Section 7.4.

4.1.1. Weakening Of Cryptographic Algorithms And Parameters

Cryptographic algorithms and parameters will be broken or weakened over time. Blindly implementing cipher suites listed in the registries is not advised.

Implementers and users *SHOULD* check that the cryptographic algorithms listed continue to provide the expected level of security.

4.2. Interoperability Recommendations

Recommendations for interoperability are generally less urgent but greatly beneficial for the OpenPGP user experience.

The following registries shall have the "Interoperability Recommendation" column added:

- PGP String-to-Key (S2K) Registry
- PGP Packet Types/Tags Registry
- PGP User Attribute Types Registry

- Image Format Subpacket Types Registry
- Signature Subpacket Types Registry
- Key Server Preference Extensions Registry
- Reason for Revocation Extensions Registry
- Implementation Features Registry
- New Packet Versions Registry
- Key Flags Extensions Registry
- Public Key Algorithms Registry
- Symmetric Key Algorithms Registry
- Hash Algorithms Registry
- Compression Algorithms Registry

The allowed values for this column are:

- Yes: Recommended, implementation of this feature enhances interoperability for OpenPGP;
- No: Not recommended, implementation of this feature reduces interoperability for OpenPGP;
- Empty: No comment, there is no recommendation on this feature on interoperability.

An "Interoperability Recommendation" *MUST* only be accepted through an Expert Review described in Section 7.4.

4.3. No Recommendation

An item not marked as "Recommended" does not mean it is "Not Recommended". This could simply be a reflection that this item has not been through Expert Review, has limited applicability, is intended only for specific use cases, or for other reasons.

Not all newly defined parameters in a Standards Track document need to be marked as "Recommended".

5. IANA OpenPGP Registries

5.1. PGP String-to-Key (S2K) Registry

Proposed changes to the registry:

- Rename the registry to "OpenPGP String-to-Key (S2K) Algorithms"
- Change registry policy to *Specification Required*.
- Update its "Reference" to also refer to this document.
- A Standards Track document is required to register an S2K algorithm with the value "Yes" in any recommendation.

Add the following note:

Note: Experts are to verify that the proposed registration provides a publicly-available standard that can be implemented in an interoperable way, with notable benefits for the wider OpenPGP community.

Update the following registrations:

ID	S2K Type	REC-S	REC-I	Reference
0	Simple S2K	No	Yes	Section 3.7.1.1 of [RFC4880]
1	Salted S2K	No	Yes	Section 3.7.1.2 of [RFC4880]
2	Reserved			Section 3.7.1 of [RFC4880]
3	Iterated and Salted S2K	Yes	Yes	Section 3.7.1.3 of [RFC4880]
4-99	Unassigned			
100-110	Private or Experimental Use			Section 3.7.1 of [RFC4880]
111-255	Unassigned			

5.2. PGP Packet Types/Tags Registry

Proposed changes to the registry:

- Rename the registry to "OpenPGP Packet Types"
- Rename the column "Attribute" to "Packet Type"

- Change registry policy to *RFC Required*.

- Update its "Reference" to also refer to this document.

- A Standards Track document is required to register a Packet Type with the value "Yes" in any recommendation.

Add the following note:

Note: Due to the scarcity of codepoints in this registry, experts are to verify that the proposed registration **MUST** provide notable benefits for the wider OpenPGP community, and provides a publicly-available standard that can be implemented in an interoperable way.

Update the following registrations:

Value	Packet Type	REC-S	REC-I	Reference
0	Reserved - a packet tag *MUST NOT* have this value	No	Yes	[RFC4880]
1	Public-Key Encrypted Session Key Packet	Yes	Yes	[RFC4880]
2	Signature Packet	Yes	Yes	[RFC4880]
3	Symmetric-Key Encrypted Session Key Packet	Yes	Yes	[RFC4880]
4	One-Pass Signature Packet	Yes	Yes	[RFC4880]
5	Secret Key Packet	Yes	Yes	[RFC4880]
6	Public Key Packet	Yes	Yes	[RFC4880]
7	Secret Subkey Packet	Yes	Yes	[RFC4880]
8	Compressed Data Packet	Yes	Yes	[RFC4880]
9	Symmetrically Encrypted Data Packet	No	Yes	[RFC4880]
10	Marker Packet	No	No	[RFC4880]
11	Literal Data Packet	No	Yes	[RFC4880]
12	Trust Packet		No	[RFC4880]
13	User ID Packet		Yes	[RFC4880]
14	Public Subkey Packet	Yes	Yes	[RFC4880]
15-16	Unknown			[RFC4880]
17	User Attribute Packet		Yes	[RFC4880]
18	Sym. Encrypted and Integrity Protected Data Packet	Yes	Yes	[RFC4880]
19	Modification Detection Code Packet	Yes	Yes	[RFC4880]
20-59	Unassigned			
60-63	Private or Experimental Use			[RFC4880]

5.3. PGP User Attribute Types Registry

Proposed changes to the registry:

- Rename the registry to "OpenPGP User Attribute Subpacket Types"
- Rename the column "Attribute" to "User Attribute Type"
- Change registry policy to *Specification Required*.
- Update its "Reference" to also refer to this document.
- A Standards Track document is required to register an Attribute Type algorithm with the value "Yes" in any recommendation.

Add the following note:

Note: Experts are to verify that the proposed registration **SHOULD** provide notable benefits for the wider OpenPGP community, and provides a publicly-available standard that can be implemented in an interoperable way.

Update the following registrations:

Value	Attribute Type	REC-I	Reference
0	Reserved		[RFC4880]
1	image	Yes	[RFC4880]
2-99	Unassigned		
100-110	Private or Experimental Use		[RFC4880]
111-255	Unassigned		

5.4. Image Format Subpacket Types Registry

Proposed changes to the registry:

- Rename the registry to "OpenPGP Image Format Subpacket Types"
- Rename the column "Attribute" to "Image Format Type"
- Change registry policy to *Specification Required*.
- Update its "Reference" to also refer to this document.
- A Standards Track document is required to register a Packet Type/ Tag with the value "Yes" in any recommendation.

Add the following note:

Note: Experts are to verify that the proposed registration **SHOULD** provide notable benefits for the wider OpenPGP community, and provides a publicly-available standard that can be implemented in an interoperable way.

Update the following registrations:

Value	Image Format Type	REC-I	Reference
0	Reserved		[RFC4880]
1	JPEG	Yes	[RFC4880]
2-99	Unassigned		
100-110	Private or Experimental Use		[RFC4880]
111-255	Unassigned		

5.5. Signature Subpacket Types Registry

Proposed changes to the registry:

- Rename the registry to "OpenPGP Signature Subpacket Types".
- Rename the column "Attribute" to "Signature Subpacket Type"
- Change registry policy to *Specification Required*.
- Update its "Reference" to also refer to this document.
- A Standards Track document is required to register a Signature Subpacket Type with the value "Yes" in any recommendation.

Add the following note:

Note: Experts are to verify that the proposed registration **SHOULD** provide notable benefits for the wider OpenPGP community, and provides a publicly-available standard that can be implemented in an interoperable way.

Update the following registrations:

Value	Image Format Type	REC-I	Reference
0-1	Reserved		[RFC4880]
2	Signature Creation Time	Yes	[RFC4880]
3	Signature Expiration Time	Yes	[RFC4880]
4	Exportable Certification	Yes	[RFC4880]
5	Trust Signature	Yes	[RFC4880]
6	Regular Expression		[RFC4880]
7	Revocable	Yes	[RFC4880]
8	Reserved		[RFC4880]
9	Key Expiration Time	Yes	[RFC4880]
11	Preferred Symmetric Algorithms	Yes	[RFC4880]
12	Revocation Key	Yes	[RFC4880]
13-15	Reserved		[RFC4880]
16	Issuer Key ID	Yes	[RFC4880]
17-19	Reserved		[RFC4880]
20	Notation Data	Yes	[RFC4880]
21	Preferred Hash Algorithms	Yes	[RFC4880]
22	Preferred Compression Algorithms	Yes	[RFC4880]
23	Key Server Preferences		[RFC4880]
24	Preferred Key Server		[RFC4880]
25	Primary User ID	Yes	[RFC4880]
26	Policy Uri		[RFC4880]
27	Key Flags	Yes	[RFC4880]
28	Signer's User ID	Yes	[RFC4880]
29	Reason For Revocation	Yes	[RFC4880]
30	Features	Yes	[RFC4880]
31	Signature Target	Yes	[RFC4880]
32	Embedded Signature	Yes	[RFC4880]
33-99	Unassigned		[RFC4880]
100-110	Private or Experimental Use		[RFC4880]
111-127	Unassigned		

5.6. Signature Notation Data Subpacket Notation Types Registry

This registry is currently empty.

However, the existing IANA registry contains an erroneous note that the registry is about "User Notations". According to [RFC4880] which defined this registry, "[n]otations contain a user space that is completely unmanaged". This registry should be for the [RFC4880] "IETF (name)space".

Proposed changes to the registry:

- Rename the registry to "OpenPGP Notation Data Subpacket Notation Types".
- Change registry policy to *Specification Required*.
- Update its "Reference" to also refer to this document.

Update its erroneous "Note" that says:

> Notation names are arbitrary strings encoded in UTF-8. They reside two name spaces: The IETF name space and the user name space.
>
> The IETF name space is registered with IANA. These names MUST NOT contain the "@" character (0x40). This is a tag for the user name space.

To:

> Notation names are arbitrary strings encoded in UTF-8, and there are two namespaces:
>
> * IETF namespace: keys are of any string but **MUST NOT** contain the "@" character (0x40). Allowed keys **MUST** by registered in this registry.
>
> * User namespace: keys are of form "[name]@[domain]", these are unmanaged keys and NOT maintained by this registry.
>
> Note: Experts are to verify that the proposed registration is necessary and **SHOULD** provide general benefits for the wider OpenPGP community.

5.7. Key Server Preference Extensions Registry

Proposed changes to the registry:

- Rename the registry to "OpenPGP Key Server Preferences"
- Rename the column "First octet" to "Flag"
- Add a column "Octet Ordinal" to indicate the ordinal of the octet of which the "Flag" field is read from.
- Rename the column "Extension" to "Description"
- Change registry policy to *Specification Required*.
- Update its "Reference" to also refer to this document.

- A Standards Track document is required to register an item with the value "Yes" in any recommendation.

Add the following note:

This is a variable-length bit field.

Note: Experts are to verify that the proposed registration **SHOULD** provide notable benefits for the wider OpenPGP community, and provides a publicly-available standard that can be implemented in an interoperable way.

Update existing registrations:

Octet Ordinal	Flag	Description	REC-I	Reference
1	0x01	Unassigned		
1	0x02	Unassigned		
1	0x04	Unassigned		
1	0x08	Unassigned		
1	0x10	Unassigned		
1	0x20	Unassigned		
1	0x40	Unassigned		
1	0x80	No-Modify	Yes	Section 5.3.2.17 of [RFC4880]
2-		Unassigned		

5.8. Reason for Revocation Extensions Registry

Proposed changes to the registry:

- Rename the registry to "OpenPGP Reasons for Revocation"
- Rename the column "Flag" to "Reason"
- Change registry policy to *Specification Required*.
- Update its "Reference" to also refer to this document.
- A Standards Track document is required to register an item with the value "Yes" in any recommendation.
- Add the following note:

Note: Experts are to verify that the proposed registration **SHOULD** provide notable benefits for the wider OpenPGP community, and provides a publicly-available standard that can be implemented in an interoperable way.

Update the following registrations:

Value	Reason	REC-I	Reference
0	No reason specified (key revocations or cert revocations)	Yes	Section 5.2.3.23 of [RFC4880]
1	Key is superseded (key revocations)	Yes	Section 5.2.3.23 of [RFC4880]
2	Key material has been compromised (key revocations)	Yes	Section 5.2.3.23 of [RFC4880]
3	Key is retired and no longer used (key revocations)	Yes	Section 5.2.3.23 of [RFC4880]
4-31	Unassigned		Section 5.2.3.23 of [RFC4880]
32	User ID information is no longer valid (cert revocations)	Yes	Section 5.2.3.23 of [RFC4880]
33-99	Unassigned		
100-110	Private Use		Section 5.2.3.23 of [RFC4880]
111-255	Unassigned		

5.9. Implementation Features Registry

Proposed changes to the registry:

- Rename the registry to "OpenPGP Features"
- Mark value "First Octet, 0x80" as "Private Use" in the registry.
- Rename the column "Value" to "Flag"
- Add a column "Octet Ordinal" to indicate the ordinal of the octet of which the "Flag" field is read from.

- Change registry policy to *Specification Required*.
- Update its "Reference" to also refer to this document.
- A Standards Track document is required to register an item with the value "Yes" in any recommendation.

Add the following note:

This is a variable-length bit field.

Note: Experts are to verify that the proposed registration **SHOULD** provide notable benefits for the wider OpenPGP community, and provides a publicly-available standard that can be implemented in an interoperable way.

Update the following registrations:

Octet Ordinal	Flag	Feature	REC-S	REC-I	Reference
1	0x01	Modification Detection (packets 18 and 19)	Yes	Yes	Section 5.2.3.24 of [RFC4880]
1	0x02	Unassigned			
1	0x04	Unassigned			
1	0x08	Unassigned			
1	0x10	Unassigned			
1	0x20	Unassigned			
1	0x40	Unassigned			
1	0x80	Unassigned			
2-		Unassigned			

5.10. New Packet Versions Registry

This registry is currently empty.

Proposed changes to the registry:

- Rename the registry to "OpenPGP Packet Type Versions"
- It should have the following columns: "Packet Type", "Version", "Security Recommended", "Interoperability Recommended", "Reference"

- Change registry policy to *RFC Required*.

- Update its "Reference" to also refer to this document.

- Add the following note:

Note: Experts are to verify that the proposed registration **SHOULD** provide notable benefits for the wider OpenPGP community, and provides a publicly-available standard that can be implemented in an interoperable way.

- A Standards Track document is required to register a Packet Type with the value "Yes" in any recommendation.

Add in the existing (but missing) registrations:

Packet Type	Version	REC-S	REC-I	Reference
1	3	Yes	Yes	Section 5.1 of [RFC4880]
2	3	No	Yes	Section 5.2.2 of [RFC4880]
2	4	Yes	Yes	Section 5.2.3 of [RFC4880]
3	4	Yes	Yes	Section 5.3 of [RFC4880]
4	3	Yes	Yes	Section 5.4 of [RFC4880]
5	3	Yes	Yes	Section 5.5.1.3 of [RFC4880]
5	4	Yes	Yes	Section 5.5.1.3 of [RFC4880]
6	3	Yes	Yes	Section 5.5.1.1 of [RFC4880]
6	4	Yes	Yes	Section 5.5.1.1 of [RFC4880]
7	3	Yes	Yes	Section 5.5.1.4 of [RFC4880]
7	4	Yes	Yes	Section 5.5.1.4 of [RFC4880]
14	3	Yes	Yes	Section 5.5.1.2 of [RFC4880]
14	4	Yes	Yes	Section 5.5.1.2 of [RFC4880]
18	1	Yes	Yes	Section 5.13 of [RFC4880]

5.11. Key Flags Extensions Registry

Proposed changes to the registry:

- Rename the registry to "OpenPGP Key Flags"
- Rename the column "Value" to "Flag"
- Add a column "Octet Ordinal" to indicate the ordinal of the octet of which the "Flag" field is read from.
- Rename the column "Extension" to "Description"
- Mark value "First Octet, 0x40" as "Unassigned" in the registry.
- Remove ending periods for all values in "Description" for consistency with other registries.
- Change registry policy to *Specification Required*.
- Update its "Reference" to also refer to this document.
- A Standards Track document is required to register an item with the value "Yes" in any recommendation.

Add the following note:

This is a variable-length bit field.

Note: Experts are to verify that the proposed registration **SHOULD** provide notable benefits for the wider OpenPGP community, and provides a publicly-available standard that can be implemented in an interoperable way.

Update existing registrations:

Octet Ordinal	Flag	Description	REC-I	Reference
1	0x01	This key may be used to certify other keys	Yes	Section 5.2.3.21 of [RFC4880]
1	0x02	This key may be used to sign data	Yes	Section 5.2.3.21 of [RFC4880]
1	0x04	This key may be used to encrypt communications	Yes	Section 5.2.3.21 of [RFC4880]
1	0x08	This key may be used to encrypt storage	Yes	Section 5.2.3.21 of [RFC4880]
1	0x10	The private component of this key may have been split by a secret-sharing mechanism	Yes	Section 5.2.3.21 of [RFC4880]
1	0x20	This key may be used for authentication	Yes	Section 5.2.3.21 of [RFC4880]
1	0x40	Unassigned		
1	0x80	The private component of this key may be in the possession of more than one person	Yes	Section 5.2.3.21 of [RFC4880]

5.12. Public Key Algorithms Registry

Proposed changes to the registry:

- Rename registry to "OpenPGP Public Key Algorithms".
- Change registry policy to *Specification Required*.
- Update its "Reference" to also refer to this document.
- A Standards Track document is required to register an item with the value "Yes" in any recommendation.
- Existing registrations with a "Reference" value pointing to a non-IETF published document should be checked to see if an IETF-published document is available, and if so, update the reference to point to the IETF-published document instead for consistency.

Add the following note:

Note: Experts are to verify that the proposed registration **SHOULD** provide notable benefits for the wider OpenPGP community, and provides a publicly-available standard that can be implemented in an interoperable way. References to IETF-published documents are preferred. The "Reference" value should point to a document that details the implementation of this algorithm in OpenPGP, not of the algorithm itself.

Update the following registrations:

ID	Algorithm	REC-S	REC-I	Reference
1	RSA (Encrypt or Sign)	Yes	Yes	Section 13.5 of [RFC4880]
2	RSA Encrypt-Only		No	Section 13.5 of [RFC4880]
3	RSA Sign-Only		No	Section 13.5 of [RFC4880]
4-15	Unassigned			Section 13.5 of [RFC4880]
16	Elgamal (Encrypt-Only)	Yes	Yes	[RFC4880]
17	DSA (Digital Signature Algorithm)	Yes	Yes	Section 13.6 of [RFC4880]
18	ECDH public key algorithm	Yes	Yes	[RFC6637]
19	ECDSA public key algorithm	Yes	Yes	[RFC6637]
20	Reserved (formerly Elgamal Encrypt or Sign)			Section 9.1 of [RFC4880]
21	Reserved for Diffie-Hellman (X9.42, as defined for IETF-S/MIME)			Section 9.1 of [RFC4880]
22-99	Unassigned			
100-110	Private or Experimental Use			Section 13.5 of [RFC4880]
111-255	Unassigned			

5.13. Symmetric Key Algorithms Registry

Proposed changes to the registry:

- Rename registry to "OpenPGP Symmetric Key Algorithms".
- Algorithm descriptions have been simplified and applicable references moved to the "Reference" column.
- All algorithm descriptions with "[n+] bit" is updated to "[n+]-bit" for consistency, for example, the phrase "128 bit key" becomes "128-bit key".
- Change registry policy to *Specification Required*.
- Update its "Reference" to also refer to this document.
- A Standards Track document is required to register an item with the value "Yes" in any recommendation.
- Existing registrations with a "Reference" value pointing to a non-IETF published document should be checked to see if an IETF-published document is available, and if so, update the reference to point to the IETF-published document instead for consistency.

Add the following note:

Note: Experts are to verify that the proposed registration **SHOULD** provide notable benefits for the wider OpenPGP community, and provides a publicly-available standard that can be implemented in an interoperable way. References to IETF-published documents are preferred. The "Reference" value should point to a document that details the implementation of this algorithm in OpenPGP, not of the algorithm itself.

Update the following registrations:

ID	Algorithm	REC-S	REC-I	Reference
0	Plaintext		Yes	Section 13.4 of [RFC4880]
1	IDEA	No	No	Section 6.4.1 of [RFC1991]
2	TripleDES (DES-EDE, 168-bit key derived from 192-bit key)	No	Yes	Section 13.2 of [RFC4880]
3	CAST5 (128-bit key)	No	Yes	Section 9.2 of [RFC4880], [RFC2144]
4	Blowfish (128-bit key, 16 rounds)			Section 9.2 of [RFC4880]
5-6	Reserved			Section 9.1 of [RFC4880]
7	AES with 128-bit key	Yes	Yes	Section 9.2 of [RFC4880]
8	AES with 192-bit key	Yes		Section 9.2 of [RFC4880]
9	AES with 256-bit key	Yes	Yes	Section 9.2 of [RFC4880]
10	Twofish with 256-bit key			Section 9.2 of [RFC4880]
11	Camellia with 128-bit key			[RFC5581]
12	Camellia with 192-bit key			[RFC5581]
13	Camellia with 256-bit key			[RFC5581]
14-99	Unassigned			
100-110	Private or Experimental Use			Section 9.2 of [RFC4880]
111-255	Unassigned			

5.14. Hash Algorithms Registry

Proposed changes to the registry:

- Rename registry to "OpenPGP Hash Key Algorithms".
- Change registry policy to *Specification Required*.
- Update its "Reference" to also refer to this document.

- A Standards Track document is required to register an item with the value "Yes" in any recommendation.

- Existing registrations with a "Reference" value pointing to a non-IETF published document should be checked to see if an IETF-published document is available, and if so, update the reference to point to the IETF-published document instead for consistency.

Add the following note:

Note: Experts are to verify that the proposed registration **SHOULD** provide notable benefits for the wider OpenPGP community, and provides a publicly-available standard that can be implemented in an interoperable way. References to IETF-published documents are preferred. The "Reference" value should point to a document that details the implementation of this algorithm in OpenPGP, not of the algorithm itself.

Update the following registrations:

ID	Algorithm	Text Name	REC-S	REC-I	Reference
1	MD5	"MD5"	No	No	Section 9.4 of [RFC4880]
2	SHA-1	"SHA1"	No	Yes	Section 9.4 of [RFC4880]
3	RIPE-MD/160	"RIPEMD160"	Yes		Section 9.4 of [RFC4880]
4-7	Reserved				Section 9.4 of [RFC4880]
8	SHA256	"SHA256"	Yes	Yes	Section 9.4 of [RFC4880]
9	SHA384	"SHA384"	Yes		Section 9.4 of [RFC4880]
10	SHA512	"SHA512"	Yes	Yes	Section 9.4 of [RFC4880]
11	SHA224	"SHA224"	Yes		Section 9.4 of [RFC4880]
12-99	Unassigned				
	100-110	Private or Experimental Use			
Section 9.4 of [RFC4880]	111-255	Unassigned			

5.15. Compression Algorithms Registry

Proposed changes to the registry:

- Rename registry to "OpenPGP Compression Key Algorithms".
- Change registry policy to *Specification Required*.
- Update its "Reference" to also refer to this document.
- A Standards Track document is required to register an item with the value "Yes" in any recommendation.

- Existing registrations with a "Reference" value pointing to a non-IETF published document should be checked to see if an IETF-published document is available, and if so, update the reference to point to the IETF-published document instead for consistency.

Add the following note:

Note: Experts are to verify that the proposed registration **SHOULD** provide notable benefits for the wider OpenPGP community, and provides a publicly-available standard that can be implemented in an interoperable way. References to IETF-published documents are preferred.

Update the following registrations:

ID	Algorithm	REC-I	Reference
0	Uncompressed	Yes	Section 9.3 of [RFC4880]
1	ZIP	Yes	Section 9.3 of [RFC4880]
2	ZLIB	Yes	Section 9.3 of [RFC4880]
3	BZip2		Section 9.3 of [RFC4880]
4-99	Unassigned		
100-110	Private or Experimental Use		Section 9.3 of [RFC4880]
111-255	Unassigned		

5.16. New Registry: OpenPGP Signature Notation Data Subpacket Notation Flags Registry

This registry is created in accordance with Section 5.2.3.16 of [RFC4880].

The registry:

- Contain the columns "Flag", "Description", "Security Recommended", "Interoperability Recommended", Reference"

- Registry policy is *Specification Required*.

- Its "Reference" should refer to [RFC4880] and this document.

Add the following note:

This is a variable-length bit field.

Note: Experts are to verify that the proposed registration **SHOULD** provide notable benefits for the wider OpenPGP community, and provides a publicly-available standard that can be implemented in an interoperable way.

The registry *SHOULD* be initialized to the following values:

Octet Ordinal	Flag	Description	REC-S	REC-I	Reference
1	0x01	Unassigned.			Section 5.2.3.16 of [RFC4880]
1	0x02	Unassigned.			Section 5.2.3.16 of [RFC4880]
1	0x04	Unassigned.			Section 5.2.3.16 of [RFC4880]
1	0x08	Unassigned.			Section 5.2.3.16 of [RFC4880]
1	0x10	Unassigned.			Section 5.2.3.16 of [RFC4880]
1	0x20	Unassigned.			Section 5.2.3.16 of [RFC4880]
1	0x40	Unassigned.			Section 5.2.3.16 of [RFC4880]
1	0x80	This note value is human-readable text.		Yes	Section 5.2.3.16 of [RFC4880]

6. Registries With The "Specification Required" Policy

Registration requests for a *Specification Required* and *Expert Review* registry must be submitted to the Expert Pool (Section 7) through the openpgp-reg-review@ietf.org mailing list.

The registration request will be deemed successful after three approved Expert Reviews (Section 7.4), and the Designated Experts will request IANA to register the proposed registration.

6.1. Registration Request Procedure

Registration requests sent to the mailing list for review *SHOULD* use an appropriate subject (e.g., "Registration request: new algorithm in Symmetric Encryption registry").

Within the review period, the Designated Experts will either approve or deny the registration request, communicating this decision to the review list and IANA.

6.2. Registration Request Outcome

An outcome of a registration request is determined by results of Expert Reviews (Section 7.4).

A registration request is approved once it receives a minimum of three Expert Reviews that result in approval.

The outcomes of a request review are:

- Approval: once there are three approved Designated Expert reviews within the review period;

- Denial: there have been more than three Designated Expert reviews within the review period but have not met the approval threshold of three approvals.

6.3. Temporary Registrations

To allow for the allocation of values prior to publication, Designated Experts *MAY* approve a temporary registration once they are satisfied that such a specification will be published.

This temporary registration has a 1 year validity, of which when expired will be automatically revoked.

Once the specification that the proposal relies is published within this period, the Designated Experts *SHOULD* request IANA to convert this registration to an official one.

7. Designated Experts

Designated Experts are responsible for performing registration request reviews for *Expert Review* and *Specification Required* IANA OpenPGP registries.

7.1. IANA Registration

IANA *MUST* only accept registry updates from the Designated Experts and *SHOULD* direct all requests for registration to the review mailing list.

7.2. Eligibility Criteria

A Designated Expert *SHOULD* have a thorough understanding, demonstrated knowledge and experience of OpenPGP [RFC4880] and its Standards Track extensions.

7.3. Selection Criteria And Pool

Designated Experts are judged and selected by the IETF Area Director of which the "openpgp" workgroup belongs.

The selected pool of Designated Experts *SHOULD* be able to represent the perspectives of different applications using this specification, in order to enable broadly informed review of registration decisions.

7.4. Designated Expert Review

7.4.1. Review Procedure

On submission of a review request, five Designated Experts are sought out for the review of the request. These Designated Experts must provide a review decision response within 21 days of submission.

If less than three Designated Experts have performed a review by the end of that period, an extension of 21 days will be granted and extra Designated Experts selected to complete the review.

In cases where a review assignment could be perceived as creating a conflict of interest for a particular Designated Expert, that Designated Expert *SHOULD* defer review responsibility to another Designated Expert, as described in Section 5.2 of [RFC8126].

7.4.2. Review Criteria

A Designated Expert *MUST* take the following criteria into account when reviewing registration requests.

For *Specification Required* registries:

- whether the proposed registration duplicates existing functionality;

- the clarity of the proposed registration description;
- whether the specification of the proposed registration item is publicly available;
- whether the proposed registration would affect the security of users of OpenPGP; and
- whether the proposed registration is likely to be of general applicability.

7.5. Review Outcomes

Approvals *MUST* include an explanation.

Denials *MUST* include an explanation and, if applicable, constructive suggestions as to how to make the request successful.

A Designated Expert *MAY* elect to provide more in depth reviews than required. Their review should not be taken as an endorsement of the feature or underlying primitives, such as cryptographic algorithms used by a registration.

7.6. Review Appeals

The review appeals process is in accordance with 10 [RFC8126], which specifies that the normal IETF appeals process as described in Section 6.5 of [RFC2026] should be followed.

Review appeals *SHOULD* be directly brought to the IESG for resolution through the iesg@ietf.org mailing list.

The following issues are eligible for the appeals process:

- Registration requests that have not received any Designated Expert reviews for a period longer than 21 days.
- A review was performed by an inappropriate Designated Expert, for example, who is strongly suspected of a conflict of interest or has demonstrated unprofessional behavior or impartiality.

8. Security Considerations

The change to *Specification Required* from *IETF Review* lowers the barrier to add functionality and cryptographic algorithms for OpenPGP.

For registries that involve cryptographic algorithms, this change reflects the practical reality in that the "openpgp" mailing list is not responsible for cryptographic reviews, which is especially difficult for national cipher suites.

Security Recommended algorithms are regarded as secure for general use at the time of registration. However, since cryptographic algorithms and parameters will be broken or weakened over time, it *MAY* be possible that the recommended status in the registry lags behind the most recent advances in cryptanalysis. Implementers and users *SHOULD* check that the cryptographic algorithms listed continue to provide the expected level of security desired.

9. IANA Considerations

This document specifies a number of changes to the IANA OpenPGP registries.

10. Acknowledgements

The authors would like to thank the following individuals for making this document possible:

- Security Area Directors: Eric Rescola and Kathleen Moriarty;
- The inaugural SECDISPATCH chairs: Tim Polk, Nancy Cam-Winget and Russ Housley;
- Supporters of this revision scheme: Rich Salz, Sean Leonard, Richard Barnes, and Daniel Kahn Gillmor.

11. References

11.1. 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/info/rfc2119>.

[RFC4880] Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R. Thayer, "OpenPGP Message Format", RFC 4880, DOI 10.17487/RFC4880, November 2007, <https://www.rfc-editor.org/info/rfc4880>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

11.2. Informative References

[I-D.ietf-tls-iana-registry-updates]
Salowey, J. and S. Turner, "IANA Registry Updates for TLS and DTLS", draft-ietf-tls-iana-registry-updates-02 (work in progress), October 2017.

[RFC1991] Atkins, D., Stallings, W., and P. Zimmermann, "PGP Message Exchange Formats", RFC 1991, DOI 10.17487/RFC1991, August 1996, <https://www.rfc-editor.org/info/rfc1991>.

[RFC2026] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, DOI 10.17487/RFC2026, October 1996, <https://www.rfc-editor.org/info/rfc2026>.

[RFC2144] Adams, C., "The CAST-128 Encryption Algorithm", RFC 2144, DOI 10.17487/RFC2144, May 1997, <https://www.rfc-editor.org/info/rfc2144>.

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", RFC 2434, DOI 10.17487/RFC2434, October 1998, <https://www.rfc-editor.org/info/rfc2434>.

[RFC2440] Callas, J., Donnerhacke, L., Finney, H., and R. Thayer, "OpenPGP Message Format", RFC 2440, DOI 10.17487/RFC2440, November 1998, <https://www.rfc-editor.org/info/rfc2440>.

[RFC5581] Shaw, D., "The Camellia Cipher in OpenPGP", RFC 5581, DOI 10.17487/RFC5581, June 2009, <https://www.rfc-editor.org/info/rfc5581>.

[RFC6194] Polk, T., Chen, L., Turner, S., and P. Hoffman, "Security Considerations for the SHA-0 and SHA-1 Message-Digest Algorithms", RFC 6194, DOI 10.17487/RFC6194, March 2011, <https://www.rfc-editor.org/info/rfc6194>.

[RFC6637] Jivsov, A., "Elliptic Curve Cryptography (ECC) in OpenPGP", RFC 6637, DOI 10.17487/RFC6637, June 2012, <https://www.rfc-editor.org/info/rfc6637>.

[SHA1-Coll]
Wang, X., Yin, Y., and H. Yu, "Finding collisions in the full SHA-1", 2005, <https://doi.org/10.1007/11535218_2>.

Author's Address

Ronald Henry Tse
Ribose
Suite 1111, 1 Pedder Street
Central, Hong Kong
Hong Kong

Email: ronald.tse@ribose.com
URI: https://www.ribose.com