

Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 8, 2020

H. Marques
pEp Foundation
B. Hoeneisen
Ucom.ch
July 07, 2019

**pretty Easy privacy (pEp): Mapping of Privacy Rating
draft-marques-pep-rating-02**

Abstract

In many Opportunistic Security scenarios end-to-end encryption is automatized for Internet users. In addition, it is often required to provide the users with easy means to carry out authentication.

Depending on several factors, each communication channel to different peers may have a different Privacy Status, e.g., unencrypted, encrypted and encrypted as well as authenticated. Even each message from/to a single peer may have a different Privacy Status.

To display the actual Privacy Status to the user, this document defines a Privacy Rating scheme and its mapping to a traffic-light semantics. A Privacy Status is defined on a per-message basis as well as on a per-identity basis. The traffic-light semantics (as color rating) allows for a clear and easily understandable presentation to the user in order to optimize the User Experience (UX).

This rating system is most beneficial to Opportunistic Security scenarios and is already implemented in several applications of pretty Easy privacy (pEp).

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 January 8, 2020.

Copyright Notice

Copyright (c) 2019 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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
1.1.	Requirements Language	4
1.2.	Terms	4
2.	Per-Message Privacy Rating	5
2.1.	Rating Codes	5
2.2.	Color Codes	5
2.3.	Surjective Mapping of Rating Codes into Color Codes . . .	6
2.4.	Semantics of Color and Rating Codes	6
2.4.1.	Red	6
2.4.2.	No Color	7
2.4.3.	Yellow	7
2.4.4.	Green	7
3.	Per-Identity Privacy Rating	8
4.	Security Considerations	8
5.	Privacy Considerations	8
6.	IANA Considerations	8
7.	Implementation Status	8
7.1.	Introduction	9
7.2.	Current software implementing pEp	9
8.	Acknowledgements	10
9.	References	10
9.1.	Normative References	10
9.2.	Informative References	10
Appendix A.	Excerpts from the pEp Reference Implementation . . .	11
A.1.	pEp rating	11
Appendix B.	Document Changelog	12
Appendix C.	Open Issues	12
	Authors' Addresses	13

1. Introduction

In many Opportunistic Security [[RFC7435](#)] scenarios end-to-end encryption is automatized for Internet users. In addition, it is often required to provide the users with easy means to carry out authentication.

Depending on several factors, each communication channel to different identities may have a different Privacy Status, e.g.

- o unreliable
- o encrypted
- o encrypted and authenticated
- o mistrusted

Even each message from or to a single peer may have a different Privacy Status.

To display the actual Privacy Status to the user, this document defines a Privacy Rating scheme and its mapping to a traffic-light semantics, i.e., a mapping to different color codes as used in a traffic-light:

- o red
- o yellow
- o green
- o no color (or gray)

Note: While "yellow" color is used in the context of traffic-lights (e.g., in North America), in other parts of the world (e.g., the UK) this is generally referred to as "orange" or "amber" lights. For the scope of this document, "yellow", "amber", and "orange" refer to the same semantics.

A Privacy Status is defined on a per-message basis as well as on a per-identity basis. The traffic-light semantics (as color rating) allows for a clear and easily understandable presentation to the user in order to optimize the User Experience (UX). To serve also (color-)blind Internet users or those using monochrome displays, the traffic light color semantics may also be presented by simple texts and symbols for signaling the corresponding Privacy Status.

The proposed definitions are already implemented and used in applications of pretty Easy privacy (pEp) [[I-D.birk-pep](#)]. This document is targeted to applications based on the pEp framework and Opportunistic Security [[RFC7435](#)]. However, it may be also used in other applications as suitable.

Note: The pEp [[I-D.birk-pep](#)] framework proposes to automatize the use of end-to-end encryption for Internet users of email and other messaging applications and introduces methods to easily allow authentication.

[1.1.](#) Requirements Language

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](#)].

[1.2.](#) Terms

The following terms are defined for the scope of this document:

- o pEp Handshake: The process of one user contacting another over an independent channel in order to verify Trustwords (or by fallback: fingerprints). This can be done in-person or through established verbal communication channels, like a phone call. [[I-D.marques-pep-handshake](#)]
- o Trustwords: A scalar-to-word representation of 16-bit numbers (0 to 65535) to natural language words. When doing a Handshake, peers are shown combined Trustwords of both public keys involved to ease the comparison. [[I-D.birk-pep-trustwords](#)]
- o Trust On First Use (TOFU): cf. [[RFC7435](#)], which states: "In a protocol, TOFU calls for accepting and storing a public key or credential associated with an asserted identity, without authenticating that assertion. Subsequent communication that is authenticated using the cached key or credential is secure against an MiTM attack, if such an attack did not succeed during the vulnerable initial communication."
- o Man-in-the-middle (MITM) attack: cf. [[RFC4949](#)], which states: "A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association."

[2.](#) Per-Message Privacy Rating

[2.1.](#) Rating Codes

To rate messages (cf. also [Appendix A.1](#)), the following 13 Rating codes are defined as scalar values (decimal):

Rating code	Rating label
-3	under attack
-2	broken
-1	mistrust
0	undefined
1	cannot decrypt
2	have no key
3	unencrypted
4	unencrypted for some
5	unreliable
6	reliable
7	trusted
8	trusted and anonymized
9	fully anonymous

[2.2.](#) Color Codes

For an Internet user to understand what the available Privacy Status is, the following colors (traffic-light semantics) are defined:

Color code	Color label
-1	red
0	no color
1	yellow
2	green

2.3. Surjective Mapping of Rating Codes into Color Codes

Corresponding User Experience (UX) implementations use a surjective mapping of the Rating Codes into the Color Codes (in traffic light semantics) as follows:

Rating codes	Color code	Color label
-3 to -1	-1	red
0 to 5	0	no color
6	1	yellow
7 to 9	2	green

This mapping is used in current pEp implementations to signal the Privacy Status (cf. [Section 7.2](#)).

2.4. Semantics of Color and Rating Codes

2.4.1. Red

The red color MUST only be used in three cases:

- o Rating code -3: A man-in-the-middle (MITM) attack could be detected.
- o Rating code -2: The message was tempered with.
- o Rating code -1: The user explicitly states he mistrusts a peer, e.g., because a Handshake [[I-D.marques-pep-handshake](#)] mismatched or when the user learns the communication partner was attacked and might have gotten the corresponding secret key leaked.

2.4.2. No Color

No specific (or a gray color) MUST be shown in the following cases:

- o Rating code 0: A message can be rendered, but the encryption status is not clear, i.e., undefined
- o Rating code 1: A message cannot be decrypted (because of an error not covered by rating code 2 below).
- o Rating code 2: No key is available to decrypt a message (because it was encrypted with a public key for which no secret key could be found).
- o Rating code 3: A message is received or sent out unencrypted (because it was received unencrypted or there's no public key to encrypt a message to a recipient).
- o Rating code 4: A message is sent out unencrypted for some of the recipients of a group (because there's at least one recipient in the group whose public key is not available to the sender).
- o Rating code 5: A message is encrypted, but cryptographic parameters (e.g., the cryptographic method employed or key length) are insufficient.

2.4.3. Yellow

- o Rating code 6: Whenever a message can be encrypted or decrypted with sufficient cryptographic parameters, it's considered reliable. It is mapped into the yellow color code.

2.4.4. Green

- o Rating code 7: A message is mapped into the green color code only if a pEp handshake [[I-D.marques-pep-handshake](#)] was successfully carried out.

By consequence that means, that the pEp propositions don't strictly follow the TOFU (cf. [[RFC7435](#)]) approach, in order to avoid signaling trust without peers verifying their channel first.

In current pEp implementations (cf. [Section 7](#)) only rating code 7 is achieved.

The rating codes 8 and 9 are reserved for future use in pEp implementations which also secure meta-data (rating code 8), by using a peer-to-peer framework like GNUnet [[GNUnet](#)], and/or allow for fully

anonymous communications (rating code 9), where sender and receiver don't know each other, but trust between the endpoints could be established nevertheless.

3. Per-Identity Privacy Rating

The same Color Codes (red, no color, yellow and green) as for messages (cf. [Section 2.2](#)) MUST be applied for identities (peers), so that a user can easily understand, which identities private communication is possible with.

The green color code MUST be applied to an identity whom the pEp handshake [[I-D.marques-pep-handshake](#)] was successfully carried out with.

The yellow color code MUST be set whenever a public key could be obtained to securely encrypt messages to an identity, although a MITM attack cannot be excluded.

The no color code MUST be used for the case that no public key is available to engage in private communications with an identity.

The red color code MUST only be used when an identity is marked as mistrusted.

[[It's not yet clear if there are proper cases where it makes sense to set an identity automatically to the red color code, as it appears to be difficult to detect attacks (e.g., secret key leakage) at the other endpoint with certainty.]]

4. Security Considerations

[[TODO]]

5. Privacy Considerations

[[TODO]]

6. IANA Considerations

This document has no actions for IANA.

7. Implementation Status

7.1. Introduction

This section records the status of known implementations of the protocol defined by this specification at the time of posting of this Internet-Draft, and is based on a proposal described in [\[RFC7942\]](#). The description of implementations in this section is intended to assist the IETF in its decision processes in progressing drafts to RFCs. Please note that the listing of any individual implementation here does not imply endorsement by the IETF. Furthermore, no effort has been spent to verify the information presented here that was supplied by IETF contributors. This is not intended as, and must not be construed to be, a catalog of available implementations or their features. Readers are advised to note that other implementations may exist.

According to [\[RFC7942\]](#), "[...] this will allow reviewers and working groups to assign due consideration to documents that have the benefit of running code, which may serve as evidence of valuable experimentation and feedback that have made the implemented protocols more mature. It is up to the individual working groups to use this information as they see fit."

7.2. Current software implementing pEp

The following software implementing the pEp protocols (to varying degrees) already exists:

- o pEp for Outlook as add-on for Microsoft Outlook, release [\[SRC.pepforoutlook\]](#)
- o pEp for Android (based on a fork of the K9 MUA), release [\[SRC.pepforandroid\]](#)
- o Enigmail/pEp as add-on for Mozilla Thunderbird, release [\[SRC.enigmailpep\]](#)
- o pEp for iOS (implemented in a new MUA), beta [\[SRC.pepforios\]](#)

pEp for Android, iOS and Outlook are provided by pEp Security, a commercial entity specializing in end-user software implementing pEp while Enigmail/pEp is pursued as community project, supported by the pEp Foundation.

All software is available as Free Software and published also in source form.

8. Acknowledgements

The authors would like to thank the following people who have provided feedback or significant contributions to the development of this document: Leon Schumacher and Volker Birk

This work was initially created by pEp Foundation, and then reviewed and extended with funding by the Internet Society's Beyond the Net Programme on standardizing pEp. [[ISOC.bnet](#)]

9. References

9.1. Normative References

- [I-D.birk-pep]
Marques, H. and B. Hoeneisen, "pretty Easy privacy (pEp): Privacy by Default", [draft-birk-pep-03](#) (work in progress), March 2019.
- [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>>.
- [RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, [RFC 4949](#), DOI 10.17487/RFC4949, August 2007, <<https://www.rfc-editor.org/info/rfc4949>>.
- [RFC7435] Dukhovni, V., "Opportunistic Security: Some Protection Most of the Time", [RFC 7435](#), DOI 10.17487/RFC7435, December 2014, <<https://www.rfc-editor.org/info/rfc7435>>.

9.2. Informative References

- [GUnet] Grothoff, C., "The GUnet System", October 2017, <<https://grothoff.org/christian/habil.pdf>>.
- [I-D.birk-pep-trustwords]
Birk, V., Marques, H., and B. Hoeneisen, "IANA Registration of Trustword Lists: Guide, Template and IANA Considerations", [draft-birk-pep-trustwords-03](#) (work in progress), March 2019.
- [I-D.marques-pep-handshake]
Marques, H. and B. Hoeneisen, "pretty Easy privacy (pEp): Contact and Channel Authentication through Handshake", [draft-marques-pep-handshake-02](#) (work in progress), March 2019.

[ISOC.bnet]

Simao, I., "Beyond the Net. 12 Innovative Projects Selected for Beyond the Net Funding. Implementing Privacy via Mass Encryption: Standardizing pretty Easy privacy's protocols", June 2017, <<https://www.internetsociety.org/blog/2017/06/12-innovative-projects-selected-for-beyond-the-net-funding/>>.

[RFC7942] Sheffer, Y. and A. Farrel, "Improving Awareness of Running Code: The Implementation Status Section", [BCP 205](#), [RFC 7942](#), DOI 10.17487/RFC7942, July 2016, <<https://www.rfc-editor.org/info/rfc7942>>.

[SRC.enigmailpep]

"Source code for Enigmail/pEp", July 2019, <<https://enigmail.net/index.php/en/download/source-code>>.

[SRC.pepforandroid]

"Source code for pEp for Android", July 2019, <<https://pep-security.lu/gitlab/android/pep>>.

[SRC.pepforios]

"Source code for pEp for iOS", July 2019, <https://pep-security.ch/dev/repos/pEp_for_iOS/>.

[SRC.pepforoutlook]

"Source code for pEp for Outlook", July 2019, <https://pep-security.lu/dev/repos/pEp_for_Outlook/>.

[Appendix A.](#) Excerpts from the pEp Reference Implementation

This section provides excerpts of the running code from the pEp reference implementation pEp engine (C99 programming language).

[A.1.](#) pEp rating

From the reference implementation by the pEp foundation, src/message_api.h:


```
typedef enum _PEP_rating {
    PEP_rating_undefined = 0,
    PEP_rating_cannot_decrypt,
    PEP_rating_have_no_key,
    PEP_rating_unencrypted,
    PEP_rating_unencrypted_for_some,
    PEP_rating_unreliable,
    PEP_rating_reliable,
    PEP_rating_trusted,
    PEP_rating_trusted_and_anonymized,
    PEP_rating_fully_anonymous,

    PEP_rating_mistrust = -1,
    PEP_rating_b0rken = -2,
    PEP_rating_under_attack = -3
} PEP_rating;
```

[Appendix B.](#) Document Changelog

[[RFC Editor: This section is to be removed before publication]]

- o [draft-marques-pep-rating-02](#):
 - * Add Privacy and IANA Considerations sections
 - * Updated Terms
- o [draft-marques-pep-rating-01](#):
 - * Update references
 - * Minor edits
- o [draft-marques-pep-rating-00](#):
 - * Initial version

[Appendix C.](#) Open Issues

[[RFC Editor: This section should be empty and is to be removed before publication]]

- o Better explain usage of Color Codes in Per-Identity Privacy Rating
- o Decide whether rating code scalars 6 and 7-9 should be raised to leave space for future extensions
- o Add Security Considerations

- o Add more source code excerpts to Appendix
- o Add rating codes for secure cryptographic methods and parameters and reference them

Authors' Addresses

Hernani Marques
pEp Foundation
Oberer Graben 4
CH-8400 Winterthur
Switzerland

Email: hernani.marques@pep.foundation
URI: <https://pep.foundation/>

Bernie Hoeneisen
Ucom Standards Track Solutions GmbH
CH-8046 Zuerich
Switzerland

Phone: +41 44 500 52 40
Email: bernie@ietf.hoeneisen.ch (bernhard.hoeneisen AT ucom.ch)
URI: <https://ucom.ch/>

