Email, Emacs and Encryption

Abschlussvortrag

Moritz Müller Philip K.

2020/03/02

Zeitplan

Moritz

- 2-4 Behandlung von öffentlichen Schlüsseln
- 5-9 Automatische Signaturen

Philip

- 2-4 Keyserver kommunikation Umsetzen
- 5-7 Automatische Verschlüsselung
- 8-9 Bedingte Verschlüsselung

- Die meisten Aufgaben sind unabhängig voneinander bearbeitbar
- Wir zielen prinzipiell auf paralleles Arbeiten

Zeitplan

Moritz

2-4 Behandlung von öffentlichen Schlüsseln

5-9 ~~Automatische Signaturen~~

Philip

2-4 Keyserver kommunikation Umsetzen

5-7 ~~Automatische Verschlüsselung~~

8-9 ~~Bedingte Verschlüsselung~~

- Die meisten Aufgaben sind unabhängig voneinander bearbeitbar
- Wir zielen prinzipiell auf paralleles Arbeiten

Zeitplan

Moritz

2-4 Behandlung von öffentlichen Schlüsseln Tag 1-3

5-9 ~~Automatische Signaturen~~

Philip

2-4 Keyserver kommunikation Umsetzen

5-7 ~~Automatische Verschlüsselung~~

8-9 ~~Bedingte Verschlüsselung~~

- Die meisten Aufgaben sind unabhängig voneinander bearbeitbar
- Wir zielen prinzipiell auf paralleles Arbeiten

Zeitplan

Moritz

2-4 Behandlung von öffentlichen Schlüsseln Tag 1-3

5-9 ~~Automatische Signaturen~~

Philip

2-4 Keyserver kommunikation Umsetzen Tag 1-2

5-7 ~~Automatische Verschlüsselung~~

8-9 ~~Bedingte Verschlüsselung~~

- Die meisten Aufgaben sind unabhängig voneinander bearbeitbar
- Wir zielen prinzipiell auf paralleles Arbeiten

“Now what?”

Tatsächliche Zeitausnutzung (Philip)

SKS Keyserver Kommunikation (Tag 1–2)

- Implementierung des HKP Protokolls[13].
- Umsetzen einer Emacs Benutzeroberfläche[8].

Tatsächliche Zeitausnutzung (Philip)

SKS Keyserver Kommunikation (Tag 1–2)

- Implementierung des HKP Protokolls[13].
- Umsetzen einer Emacs Benutzeroberfläche[8].

Ein `keys.openpgp.org` client (Tag 2–3)

- `keys.openpgp.org` ist ein versuch Keyserver zu verbessern[9].
- `openpgp.el`[11] setzt ihr neues Protokoll um.

Tatsächliche Zeitausnutzung (Philip)

SKS Keyserver Kommunikation (Tag 1–2)

- Implementierung des HKP Protokolls[13].
- Umsetzen einer Emacs Benutzeroberfläche[8].

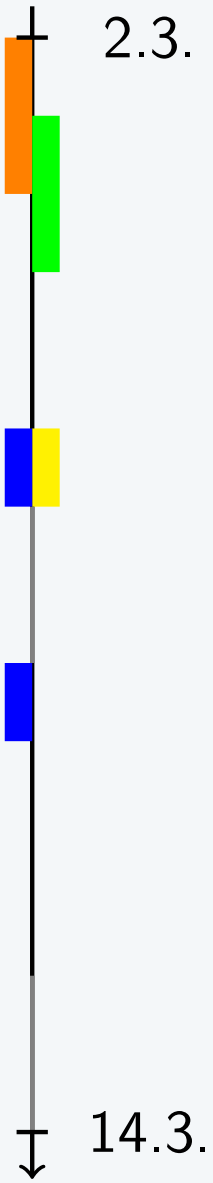
Ein `keys.openpgp.org` client (Tag 2–3)

- `keys.openpgp.org` ist ein versuch Keyserver zu verbessern[9].
- `openpgp.el`[11] setzt ihr neues Protokoll um.

`OpenPGP` Header Generierung (Tag 5)

- Ein *fast*-Standard zur Verteilung von PGP Schlüsseln[12]
- Als Patch auf der Emacs Mailing Liste eingericht[1].

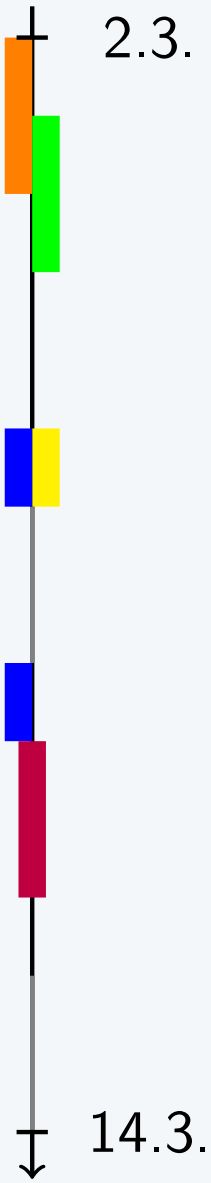
Tatsächliche Zeitausnutzung (Philip)



Libravatar[10] Unterstützung (Tag 5, 8)

- Hat eigentlich nichts mit Kryptographie zu tun, außer MD5
- Auch als Patch eingereicht[2].

Tatsächliche Zeitausnutzung (Philip)



Libravatar[10] Unterstützung (Tag 5, 8)

- Hat eigentlich nichts mit Kryptographie zu tun, außer MD5
- Auch als Patch eingereicht[2].

Autocrypt Implementierung (Tag 9–11)

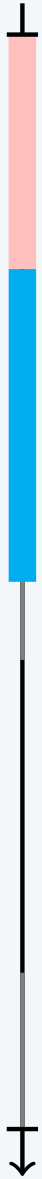
- Ein umfangreiches Umdenken vom Email/Verschlüßelungs Ansatz
- `autocrypt.el`[7] soll bald selbstständig veröffentlicht werden auf MELPA.

Tatsächliche Zeitausnutzung (Moritz)

Import von PGP Schlüsseln im Anhang (Tag 1–3)

- Beheben eines Bugs mit der Verarbeitung von Anhängen[3].
- Tatsächliche Funktion als Pull Request bei `https://github.com/djcb/mu` eingereicht[4].

Tatsächliche Zeitausnutzung (Moritz)



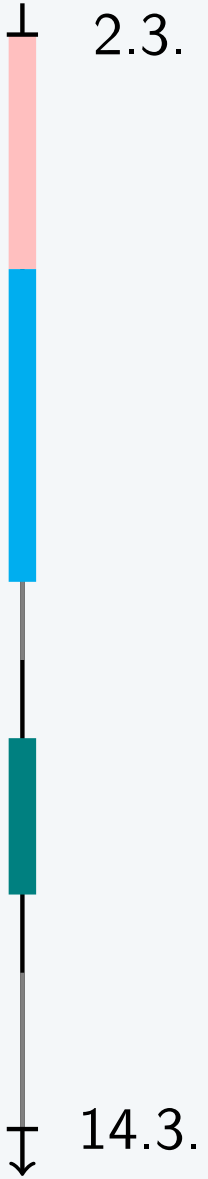
Import von PGP Schlüsseln im Anhang (Tag 1–3)

- Beheben eines Bugs mit der Verarbeitung von Anhängen[3].
- Tatsächliche Funktion als Pull Request bei `https://github.com/djcb/mu` eingereicht[4].

Umschreiben der *Crypto Policy* Option (Tag 4–8)

- Bisher war es erkenntlich wie Nachrichten automatisch verschlüßelt werden.
- Zusammengefasst *und* Erweitert in einem weiterem Pull Request[5].

Tatsächliche Zeitausnutzung (Moritz)



Import von PGP Schlüsseln im Anhang (Tag 1–3)

- Beheben eines Bugs mit der Verarbeitung von Anhängen[3].
- Tatsächliche Funktion als Pull Request bei `https://github.com/djcb/mu` eingereicht[4].

Umschreiben der *Crypto Policy* Option (Tag 4–8)

- Bisher war es erkenntlich wie Nachrichten automatisch verschlüßelt werden.
- Zusammengefasst *und* Erweitert in einem weiterem Pull Request[5].

Erweitern von mu-Core (Tag 10–11)

- Möglichkeit spezifische Header aus Nachrichten abzurufen, was bisher nicht vorhergesehen war.
- Auch als Pull Request Eingericht[6].

FAZIT

(This slide has been intentionally left (almost) blank)

Referenzen I

[1] [PATCH] Add support for creating OpenPGP header. URL: https://lists.gnu.org/archive/html/bug-gnu-emacs/2020-03/msg00265.html.

[2] [PATCH] Add support for multiple gravatar-like services. URL: https://lists.gnu.org/archive/html/bug-gnu-emacs/2020-03/msg00264.html.

[3] 1605: Fix of the attachment actions. URL: https://github.com/djcb/mu/pull/1605.

[4] 1606: Added option to attachment-options to import gpg public ke
URL: https://github.com/djcb/mu/pull/1606.

[5] 1610: Merged crypto-policy configuration into one variable. URL: https://github.com/djcb/mu/pull/1610.

Referenzen II

[6] 1614: Adding support to query the headers of a message. URL: https://github.com/djcb/mu/pull/1614.

[7] Autocrypt, Convenient End-to-End Encryption for E-Mail. URL: https://autocrypt.org/.

[8] epa-ks.el. URL: https://wwwcip.cs.fau.de/~oj14ozun/src+etc/epa-ks.el.

[9] keys.openpgp.org. URL: https://keys.openpgp.org/.

[10] Libravatar Seite. URL: https://www.libravatar.org/.

[11] openpgp.el. URL: https://wwwcip.cs.fau.de/~oj14ozun/src+etc/openpgp.el.

[12] The "OpenPGP" mail and news header field. URL: https://tools.ietf.org/html/draft-josefsson-openpgp-mailnews-header-07.

Referenzen III

[13] The OpenPGP HTTP Keyserver Protocol. URL: https://tools.ietf.org/html/draft-shaw-openpgp-hkp-00.