Much easier Email crypto, by fetching pubkey via HTTPS

How does it work?

As an email user, you just select the recipient(s) and can see that the email will be encrypted.

If you and your peers use email-providers offering this "web key service", it works by the first email. Otherwise encryption will start after you have exchanged some emails.

Technically your email client will automatically

- prepare for this by creating a crypto key for you and uploading it to your provider (or second best to public keyservers).
- sign all emails so others see that you are ready for crypto (unless you opt out)
- ask the mail provider of your recipients for their pubkeys.

An email-provider supporting privacy can

- provide a pubkey for users via HTTPS, called "web key directory" (WKD).
- allow each user's email client to automatically manage the pubkey that gets published by email, called "web key service" (WKS).

Details / Discussion

Pubkey Distribution Concept <- the (technical) details

- 2016-09-08 OpenPGP.conf presentation by Werner Koch: Abstract Slides.PDF
- 2016-09-08 OpenPGP.conf presentation by Bernhard Reiter, pages 21-24 Slides.ODP Slides.PDF
- 2016-09-09 *OpenPGP-Schlüssel über HTTPS verteilen* Golem news by Hanno Böck
- 2016-09-11 *Spezifikation für die Verteilung von OpenPGP-Keys per HTTPS veröffentlicht* Heise news by Johannes Merkert
- 2016-09-11 *Anmerkungen zum Web Key Service* gnupg-de@ by Werner Koch
- 2017-07-28 Draft 04 of the specs published (see details page linked above).

The elaborated proposal is a result of the EasyGpg2016 contract.

Implementations

Current GnuPG 2.2

- WKD lookup since v2.1.12, enabled by default since 2.1.23. Widespread rollout in 2017 because the old GnuPG 2.0 is scheduled end-of-life December 2017.
- WKS server and client tools since GnuPG v2.1.14 which may help some providers (especially smaller ones) see the Web Key Service page.

Mail User Agents

(Note that mail users agents using a modern GnuPG 2.2 will automatically do WKD requests via GnuPG. So they are WKD ready.)

Automatic pubkey bootstrapping (using the Web Key Service)

- basic (pre-release) Kontact Mail/KMail support (part of EasyGpg2016)
- basic (pre-release) Thunderbird/Enigmail support (part of EasyGpg2016)
- active consideration in planning for mutt
- active consideration in planning for GpgOL (Gpg4win's Outlook Plugin)

Mail Service Providers

- Posteo offers web key directory lookup and service for `@posteo.de` -addresses (Since 2016-12)
- (gnupg.org) Testing accounts by request for developers implementing WKS in Free Software MUAs.

- (Several smaller organisations. Like - unsurprisingly - g10code.com and intevation.de. *Let us know if you want to be publically listed.*)

WKD stand-a-lone (without WKS)

- wks-tools helps to publish a single pubkeyring via static HTTPS.