

Lightning Talk:  
«Encryption for the masses with  
pretty Easy privacy (p≡p)»  
A rough overview

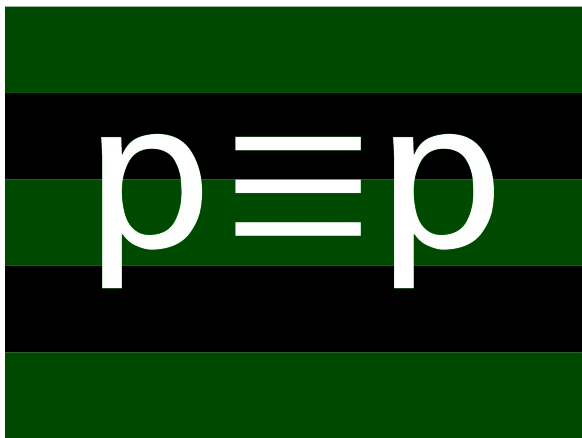
Hernâni Marques, p≡p foundation council member

FOSDEM 2017, Brussels, Feb 4th 2017, 13:40–13:55

# Overview for the next 15mins

- 1 What  $p \equiv p$  is
- 2 Motivation for  $p \equiv p$
- 3  $p \equiv p$  & OpenPGP: differences and app example
- 4 To be done
- 5 Community work
- 6 Your turn

# $p \equiv p$ = pretty Easy privacy



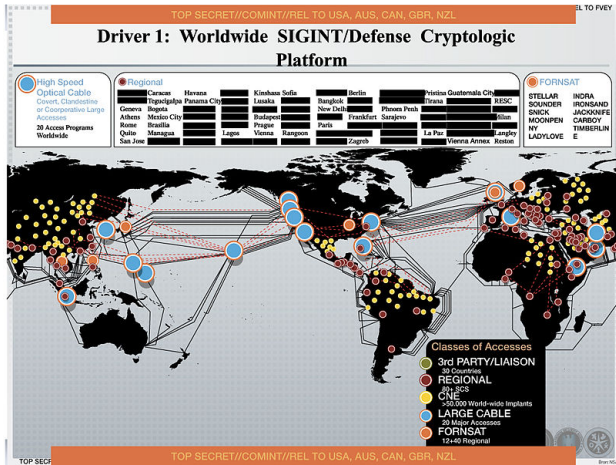
## p≡p is not . . .

- yet another crypto tool with closed (small) user base.
- a (centralized) platform provider.
- a crypto project nor implementing any own crypto.
- replacing any existing crypto tool per se.
- just for encrypting email: that's just the beginning.

## p≡p is ...

- a cross-platform abstraction to easily use crypto tools already available (like GnuPG).
- designed to encrypt digital written communications, with the starting point of email.
- built with the idea of a unified inbox in mind, so that peers can reach their friends and colleagues in one place (app).
- meant to encrypt automatically whenever and with whatever (most privacy-enhancing) crypto standard available, hence the slogan *Privacy by Default*.
- hassle-free and zero-touch when used in end-user applications.

# In a general global context . . .



Hernâni Marques, p≡p foundation council member

Lightning Talk: «Encryption for the masses with pretty Easy privacy (p≡p)»

# In a general (Swiss) local context . . .



Hernâni Marques, p≡p foundation council member

Lightning Talk: «Encryption for the masses with pretty Easy privacy (p≡p)»

# In an email context . . .

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

## Example 4

- **\$acwitems** = 'machine gun' or 'grenade' or 'AK 47'
- **\$acwpositions** = 'minister of defence' or 'defense minister'
- **\$acwcountries** = 'somalia' or 'liberia' or 'sudan'
- **\$acwbrokers** = 'south africa' or 'serbia' or 'bulgaria'
- **\$acwports** = 'rangood' or 'albasra' or 'dar es salam'

```
topic('wmd/acw/govtorgs') =  
  email_body($acwitems and $acwpositions and  
    ($acwcountries or $acwbrokers or $acwports));
```

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL



# In the context of written digital communications . . .

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

## Communication Based Contexts

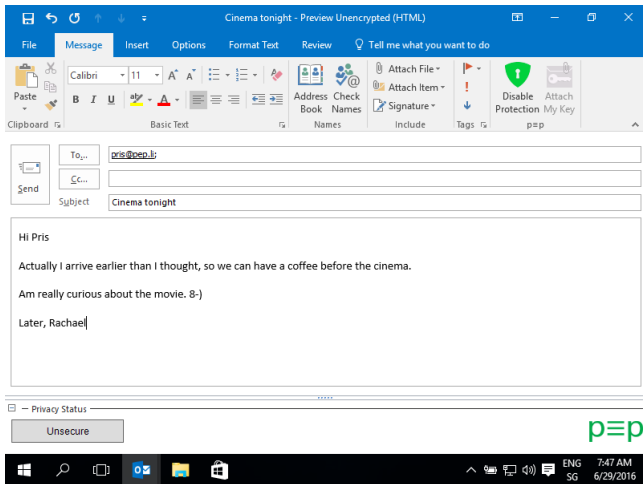
email_body(expr)	The UTF-8 normalized text of all email bodies. <a href="#">email_body('how to' and 'build' and ('bomb' or 'weapon'))</a>
chat_body(expr)	The UTF-8 normalized text of all chat bodies. <a href="#">chat_body('how to' and 'build' and ('bomb' or 'weapon'))</a>
document_body(expr)	The UTF-8 normalized text of the Office document. – Office documents include (but are not limited to) Microsoft Office, Open Office, Google Docs and Spreadsheets. <a href="#">document_body('how to' and 'build' and ('bomb' or 'weapon'))</a>
calendar_body(expr)	The UTF-8 normalized text of all calendars. An example is Google Calendar. <a href="#">calendar_body('wedding')</a>
archive_files(expr)	Matches a list of files from within an archive. For example is a ZIP file is transmitted, all names of files within are passed to this context. <a href="#">archive_files('bad.dll' or 'virus.doc')</a>
http_post_body(expr)	The UTF-8 normalized text HTTP url-encoded POSTs. <a href="#">http_post_body('action=send' and 'badguy@yahoo')</a>

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

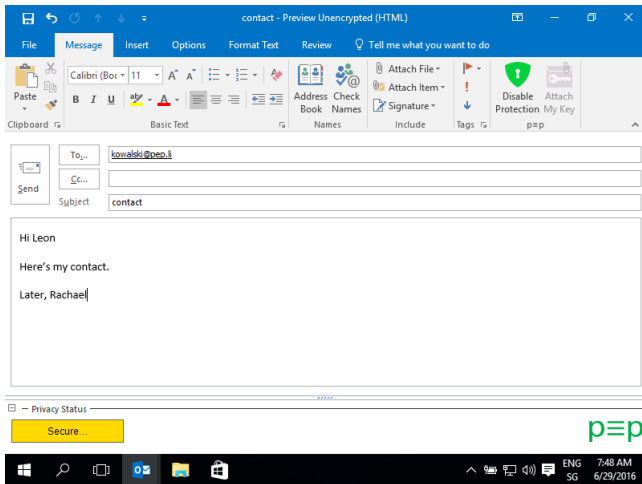
## p≡p differences to current OpenPGP MUAs

- Keyservers are never used by default to prevent leakage of a peer's social graph (by signings and queries) and MITM attacks (re-encryption).
- The sender's public key is attached by default.
- The subject field gets encrypted by default (by moving it into the body).
- Instead of fingerprints, *Trustwords* (16-bit mappings of 4-digit hexablocks to words) are used.
- p≡p has a rating system and communicates (graphically) a *Privacy Status* with traffic lights semantics to the user.

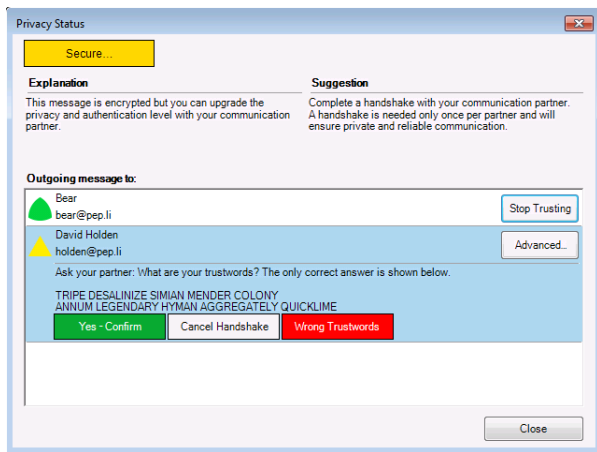
# p≡p for Outlook: first email (unsecure)



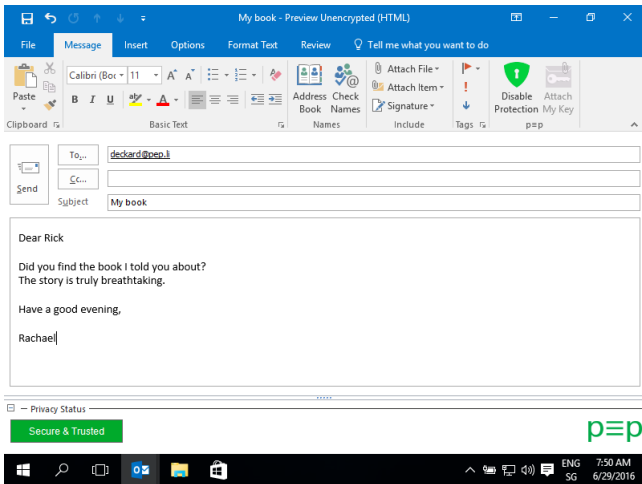
# p≡p for Outlook: second email (secure)



# p≡p for Outlook: Handshaking process



# p≡p for Outlook: third email (secure & trusted)



- Fix last bugs of the *KeySync* protocol to build device groups of a user's owned devices (i.e., read encrypted messages across devices).
- Add more message transports to p≡p engine (e.g., XMPP/OTR and as of p≡p 2.0 GNUnet).
- Implement decentralized (cloudless) synchronization of calendar and contact data through the message transport channel.
- Make p≡p an Internet standard to allow for widespread acceptance and interoperability.
- Help fight mass surveillance, also politically!

# p≡p foundation: for trust, security and community work

- The p≡p foundation is Swiss-based, tax-free (non-commercial) and controlled by privacy and digital (human) rights activists.
- The foundation holds ownership (under the GNU GPL v3) on p≡p's core (engine and adapters / bindings) and trademarks.
- We support community projects to implement p≡p and get their implementations (independently) code-audited: both support types can be of financial type.
- We also do political work and are free to support other FLOSS projects in the area of restoring Privacy, Freedom of Information and Free Speech (no strict p≡p relation needed).
- We actively collaborate with the Enigmail (on Enigmail/p≡p) & GNUnet projects and soon with ISOC Switzerland (ISOC-CH); this includes the open standardization of p≡p's protocols through the Internet community (IETF).



# Questions



Hernâni Marques, p≡p foundation council member

Lightning Talk: «Encryption for the masses with pretty Easy privacy (p≡p)»

# Aftermath

If you want to chat, share and work together: We are in building K, floor 1, group A with our friends of GNU Taler (and GNUnet) sharing a stand.