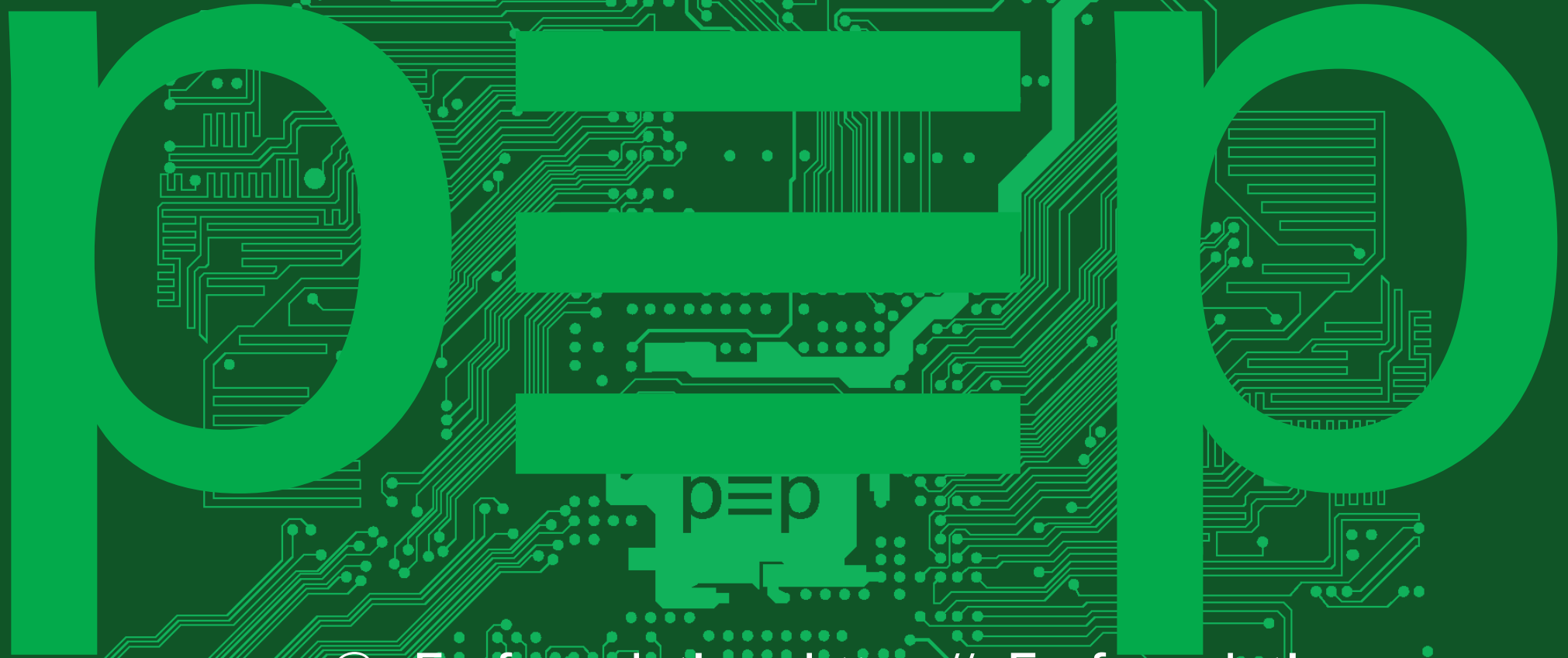


pretty Easy privacy



sva@pEp.foundation <https://pEp.foundation>
twitter@sva – twitter@pEpfoundation – #prettyeasyprivacy

Other sessions during RMLL: Wed (taler), Thu (radar)



Privacy by Default.

PGP / GPG

PGP \equiv **Pretty Good Privacy**

Created by Phil Zimmermann in 1991

see RFC 1991 (in 1996)

Zimmermann had been a long-time anti-nuclear activist, he created PGP that people might securely use BBSs and securely store messages and files

OpenPGP \equiv **standard/specification**

see RFC 2440 (in 1998) and 4880 (in 2007)

GPG \equiv **GNU Privacy Guard**

Created by Werner Koch 1999

from Free Software Foundation

(most common implementation of PGP)

Overview

- 0 – Intro
- 1 – Concept [6 sub-chapters]
- 2 – Organization
- 3 – Technology
- 4 – Apps: Current Implementation
- 5 – Apps: Demos

p≡p

0 – Intro

"I don't want to live in a world where everything that I say, everything I do, everyone I talk to, every expression of creativity or love or friendship is recorded."

(Edward Snowden)





(TS//SI//NF) PRISM Collection Details



Current Providers

What Will You Receive in Collection
(Surveillance and Stored Comms)?

It varies by provider. In general:

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple



- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

YES WE SCAN



0 – Intro: Problem & Solution

Problem:

Online communication is visible like a postcard
& this world has mass surveillance

Solution:

First: Mass encryption
Second: Mass anonymization



0 – Intro: Just a starting point...

We see ourselves as *cypherpunks* and we want to optimize the costs of mass surveillance

PGP \equiv pretty good privacy

p \equiv p \equiv pretty Easy privacy

Not only privacy for citizens,
but also security for everyone...

p \equiv p

0 – Intro: Just a starting point...

Cypherpunks?

“Privacy is necessary for an open society in the electronic age. Privacy is not secrecy.

A private matter is something one doesn’t want the whole world to know, but a secret matter is something one doesn’t want anybody to know.”



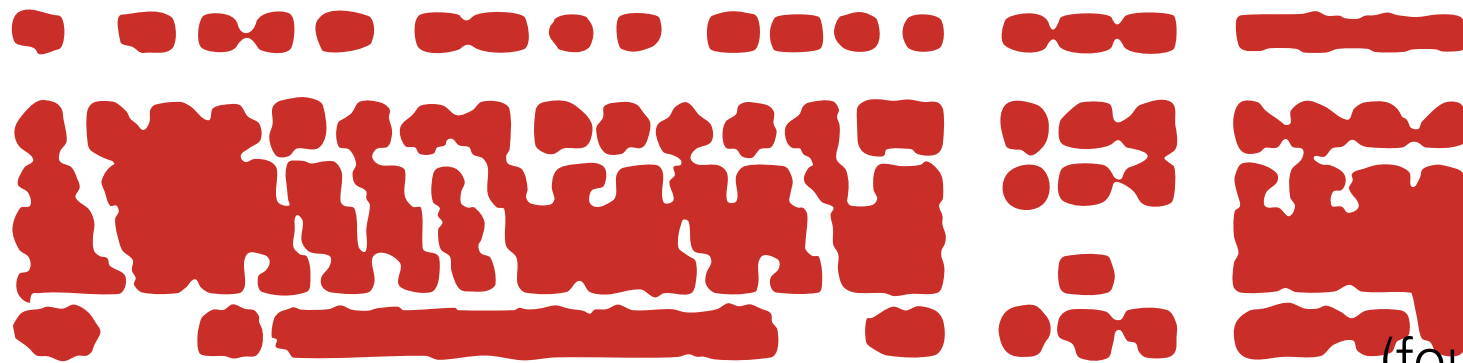
0 – Intro: sva

Anthropology

Computer science

cryptoparty.in

(l'ébéniste)



(founded 1981)

sva = unique addressing
in Internet and web

Chaos Computer Club
Hackers without Borders

(founded 2014)

p≡p

1 – Concept: Overview

1.0. Privacy by Default

1.1. pretty Easy privacy

1.2. Peer-to-Peer and End-to-End

1.3. Free Software

1.4. Compatibility (Crypto & Transports)

1.5. Anonymity (GNet)

p≡p

1.0. $p \equiv p$ Concept: Privacy by Default

Privacy by Default.

$p \equiv p$ does what the user *would want to* do

Instead of writing how-to guides
we write user expectations
into software and standards

$p \equiv p$

1.0. p≡p Concept: Privacy by Default

We started a first Internet-Draft
together with with ISOC-CH
on the general pEp principles.

It's online and ready for discussion:

<https://datatracker.ietf.org/doc/draft-birk-pep/>



Real-time
General
Internet
Ops & Mgmt
Routing
Security
Transport
IRTF

New work

Chartering groups
BOFs

Other groups

Concluded groups
Non-WG lists

Documents

Search
Draft submission
Sign in to track
docs

RFC streams

IAB
IRTF
ISE

Meetings

Agenda
Materials
Floor Plan
Past proceedings
Upcoming
Past
Request a session
Session requests

Other

IPR disclosures
Liaison
statements
IESG agenda
Downref registry
Statistics
Tutorials

Document **Type** Active Internet-Draft (individual)
Last updated 2017-06-28
Stream (None)
Intended RFC status (None)
Formats [plain text](#) [xml](#) [pdf](#) [html](#) [bibtex](#)

Stream **Stream state** (No stream defined)
Consensus Unknown
Boilerplate
RFC Editor Note (None)

IESG **IESG state** I-D Exists
Telechat date
Responsible AD (None)
Send notices to (None)

[✉ Email authors](#) [⚡ IPR](#) [← References](#) [→ Referenced by](#) [! Nits](#) [🔍 Search lists](#)

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 31, 2017
V. Birk
H. Marques
Shelburn
pEp Foundation
S. Koechli
pEp Security
June 29, 2017

pretty Easy privacy (pEp): Privacy by Default
draft-birk-pep-00

Abstract

Building on already available security formats and message transports (like PGP/MIME for email), pretty Easy privacy (pEp) describes protocols to automatize operations (key management, key discovery, private key handling including peer-to-peer synchronization of private keys and other user data across devices) that have been seen to be barriers to deployment of end-to-end secure interpersonal messaging. pEp also introduces "Trustwords" (instead of fingerprints) to verify communication peers and proposes a trust rating system to denote secure types of communications and signal the privacy level available on a per-user and per-message level. In this document, the general design choices and principles of pEp are outlined.

Status of This Memo

pep

1.0. p≡p Concept: Privacy by Default

pretty Easy privacy (pEp): Privacy by Default
draft-birk-pep-00

Abstract

Building on already available security formats and message transports (like PGP/MIME for email), pretty Easy privacy (pEp) describes protocols to automatize operations (key management, key discovery, private key handling including peer-to-peer synchronization of private keys and other user data across devices) that have been seen to be barriers to deployment of end-to-end secure interpersonal messaging. pEp also introduces "Trustwords" (instead of fingerprints) to verify communication peers and proposes a trust rating system to denote secure types of communications and signal the privacy level available on a per-user and per-message level. In this document, the general design choices and principles of pEp are outlined.

p≡p

1.0. p≡p Concept: Privacy by Default

Table of Contents

1. Introduction	3
2. Terms	4
3. Protocol's core design principles	4
3.1. Compatibility	4
3.2. Peer-to-Peer (P2P)	4
3.3. User Experience (UX)	5
4. Identities in pEp	6
5. Key Management	8
5.1. Private Keys	9
5.2. Key Distribution	10
5.3. Passphrases	11
6. Privacy Status	11
7. Options in pEp	12
7.1. Option "Passive Mode"	12
7.2. Option "Disable Protection"	12
7.2.1. For all communications	12
7.2.2. For some communications	12
7.3. Option "Extra Keys"	12
7.4. Option "Blacklist Keys"	12
7.5. Establishing trust between peers	13
8. Security Considerations	13
9. Implementation Status	13
9.1. Introduction	13
9.2. Reference implementation of pEp's core	14
9.3. Abstract Crypto API examples	15
9.3.1. Encrypting a message	15
9.3.2. Decrypting a message	16
9.3.3. Obtaining common Trustwords	17
9.4. Current software implementing pEp	18
10. Notes	19
11. Acknowledgements	19



1.1. $p \equiv p$ Concept: pretty Easy privacy

Makes Privacy Easy;
By Default.

Easy to install;
Easy to understand;
Easy to use.

No hassle; No training needed.

Also: Easy for app-devs! $p \equiv p$

1.1. Easy: Trustwords

>> **Battery Horse Staple** <<

instead of

>> **EC55 39C8 FECF** <<

p≡p

1.1. Easy: $p \equiv p$ Sync

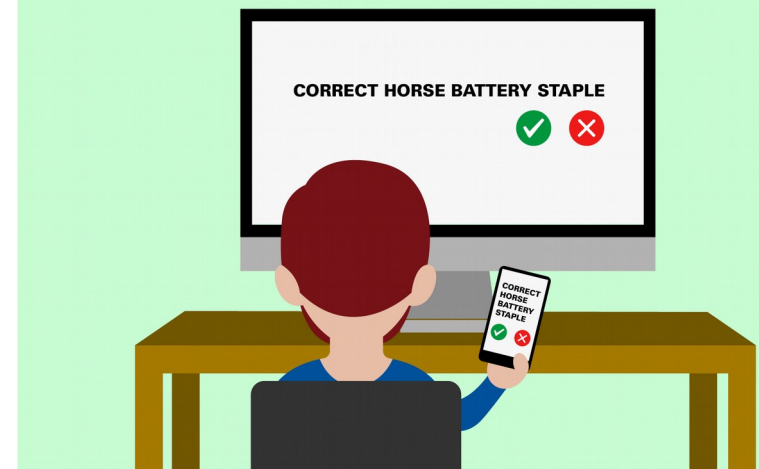
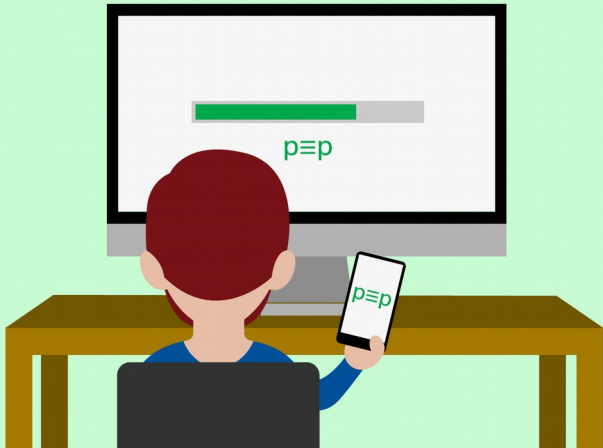
Use same keys on multiple devices:

Realized with the help of Device Groups:

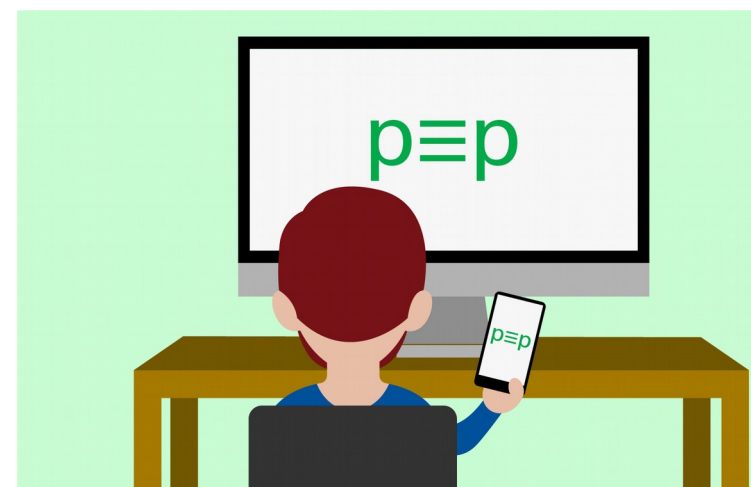
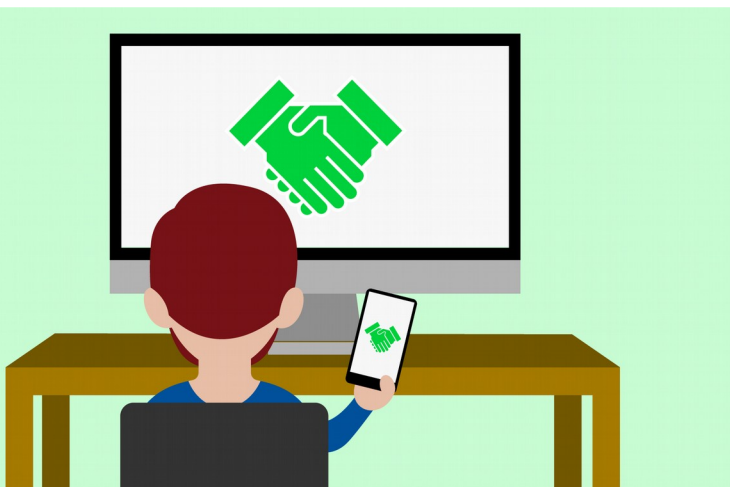
- (1) New device generates a device-key,
- (2) Pings with this one to the device-group,
- (3) Existing devices and user verify the new device,
- (4) Devices agree on a secret main group,
- (5) All Devices exchange their secret keys.

$p \equiv p$

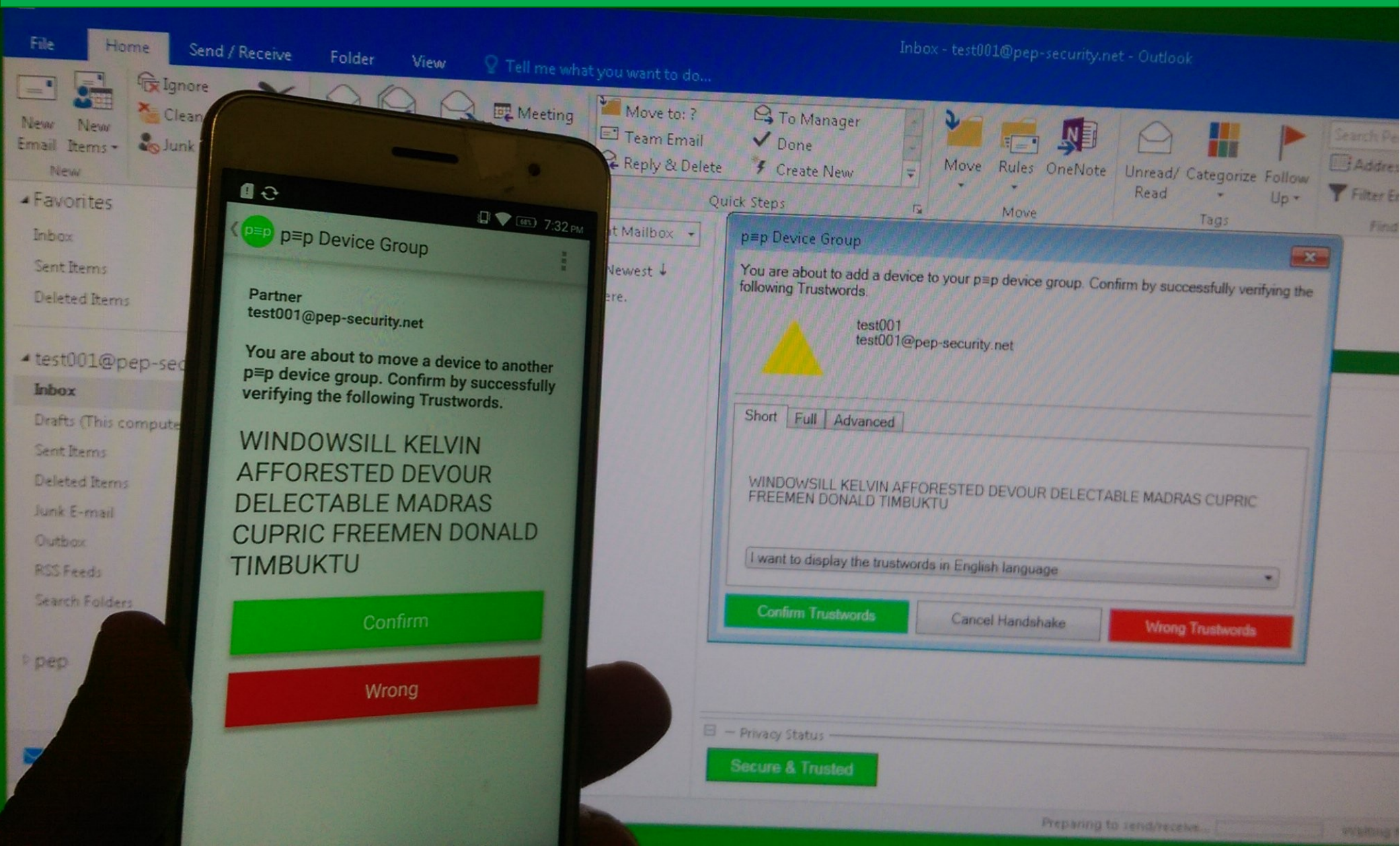
1.1. Easy: $p \equiv p$ Sync



Sync keys, contacts and calendar
(Finally the problem of backups is solved, too!)



1.1. Summary: Trustwords & p≡pSync



1.2. $p \equiv p$ Concept: Peer-to-Peer

Peer-to-peer transport

End-to-end encryption

No centralized infrastructure
or closed services

$p \equiv p$

1.3. p≡p Concept: Free Software

p≡p is Free / Libre Software

<https://pep.foundation/pep-software/>

(GPLv3)

Regular independent external
code audits



1.4. $p \equiv p$ Concept: Compatibility

Multiple crypto technologies

Multiple message transports

Multiple platforms

Multiple languages



1.4. p≡pConcept:Compatibility:Crypto

OpenPGP / GnuPG

S/MIME

OTR

OMEMO

Signal Protocol / Axolotl

...

p≡p

1.4. $p \equiv p$ Concept:Compat:Transports

SMTP / IMAP / POP3 / Exchange

XMPP (jabber)

non-open standards (e.g. Twitter DMs)

GNUnet

SMS

...

$p \equiv p$

1.5. $p \equiv p$ Concept: Anonymity

Content encryption is not everything...

E.g. E-Mail: Metadata stays visible!

(e.g.: from/to, IPs, Subject, size,...)

$p \equiv p$ already encrypts subjects inline (opt-out)

$p \equiv p$ will obfuscate & encrypt the rest of the header



1.5. $p \equiv p$ Concept: Anonymity/GNUnet

1970/80: Internet v1.0

Wow, I can access your computer, you can check out mine!!
Awesome!

2010/20: Internet v1.1

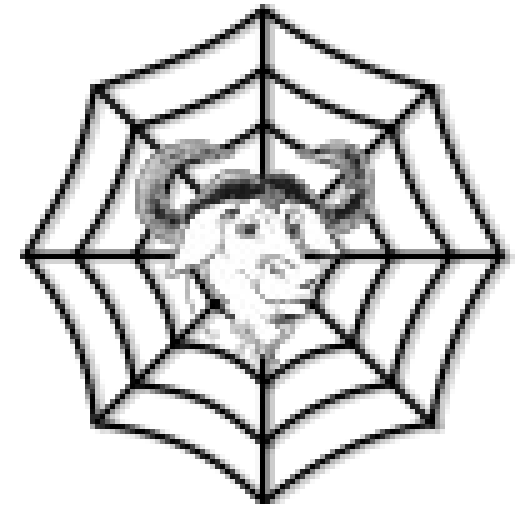
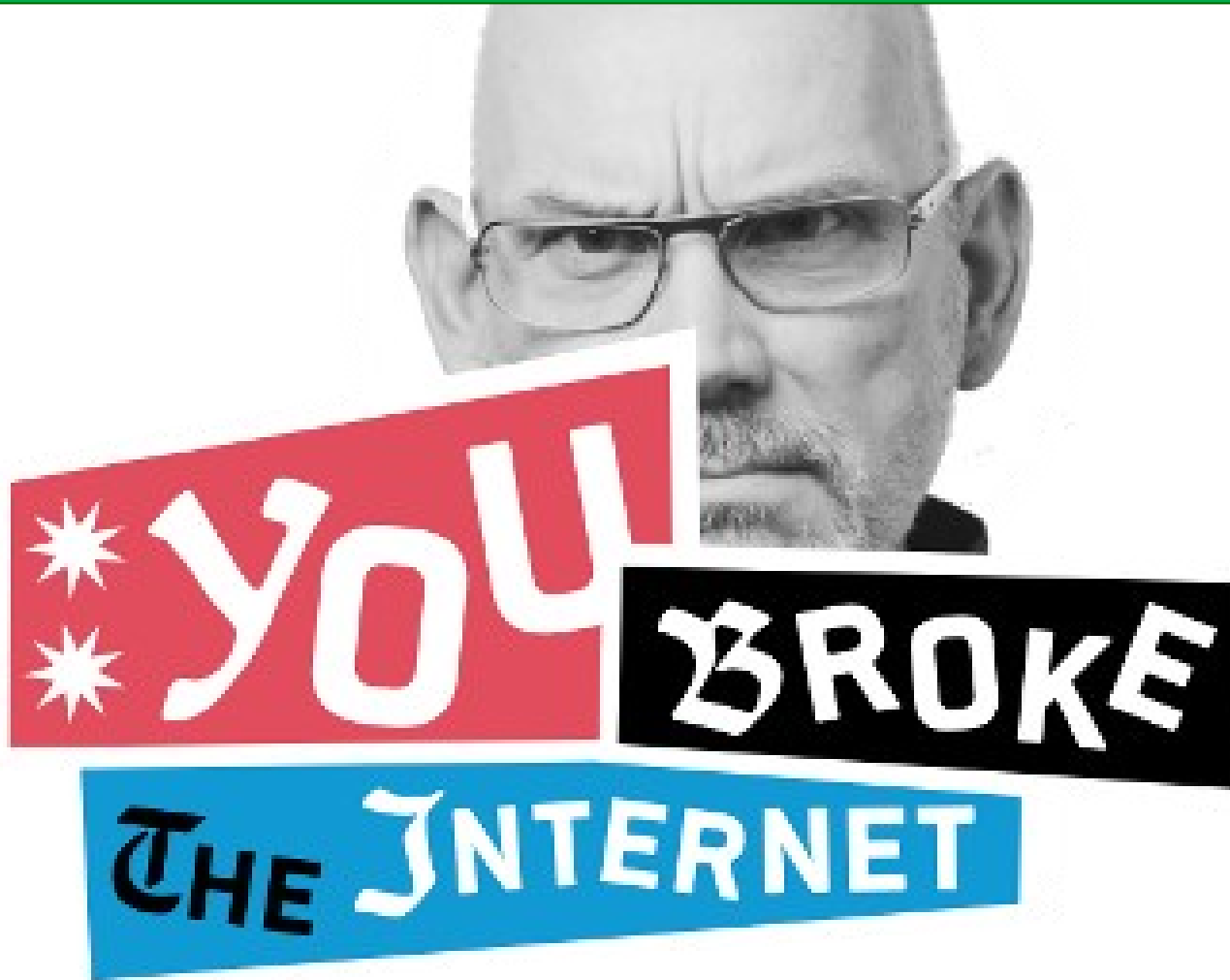
Sure I can access other computers and use their services.
Wait, What?
They can access mine!?

20xx/25: Internet v2.0

End-to-end encryption and anonymization
of the ways data flows.

$p \equiv p$

1.5. $p \equiv p$ Concept: Anonymity/GNUnet



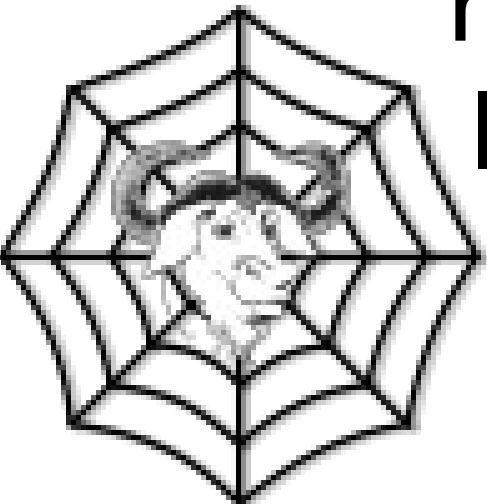
GNUnet.org

Let's make a GNU one!

$p \equiv p$

1.5. $p \equiv p$ Concept: Anonymity/GNUnet

“GNUnet is...
a mesh routing layer for
end-to-end encrypted networking and
a framework for distributed applications
designed to
replace the old insecure
Internet protocol stack.”



(started 2002 in academia)

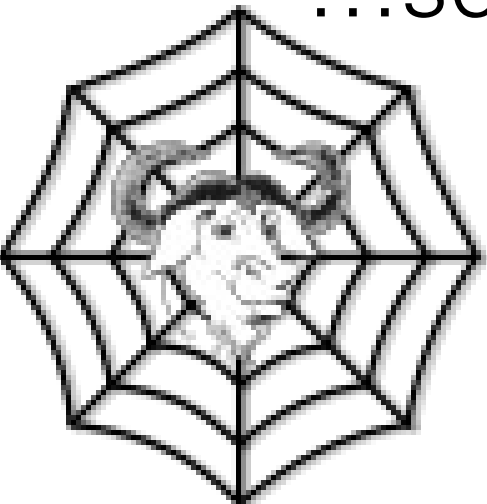
$p \equiv p$

1.5. p≡p Concept: Anonymity/GNUnet

“GNUnet wants to...

...become a widely used, reliable, open, non-discriminating, egalitarian, unfettered and censorship-resistant system of free information exchange.

...serve as a development platform for the next generation of decentralized Internet protocols.”



p≡p

1.5. $p \equiv p$ Concept: Anonymity/GNUnet

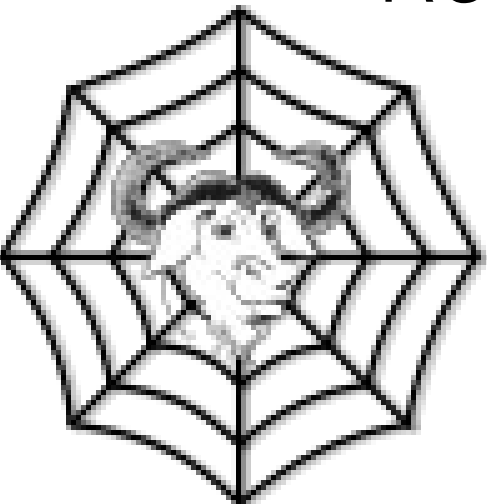
Try it out!

Clone gnunet.org/git

Follow instructions on the website

Get support via [#gnunet](#) on freenode

Report bugs on gnunet.org/bugs



$p \equiv p$

1.n. $p \equiv p$ Concept: Summary

Users don't have to think about the crypto anymore. They can just use it.

By default.

“It is this ‘little hacker inside’ that decides on the cryptography chosen to communicate with the message recipient.”

$p \equiv p$

2 – Organization: Overview

Company:

<https://prettyeasyprivacy.com/>
Sells applications and services

Foundation:

<https://pep.foundation/>
Supporting Free Software
Code belongs to the Foundation

pep

3 – Technology: Overview

3.0. Architecture

3.1. Engine and Adapters

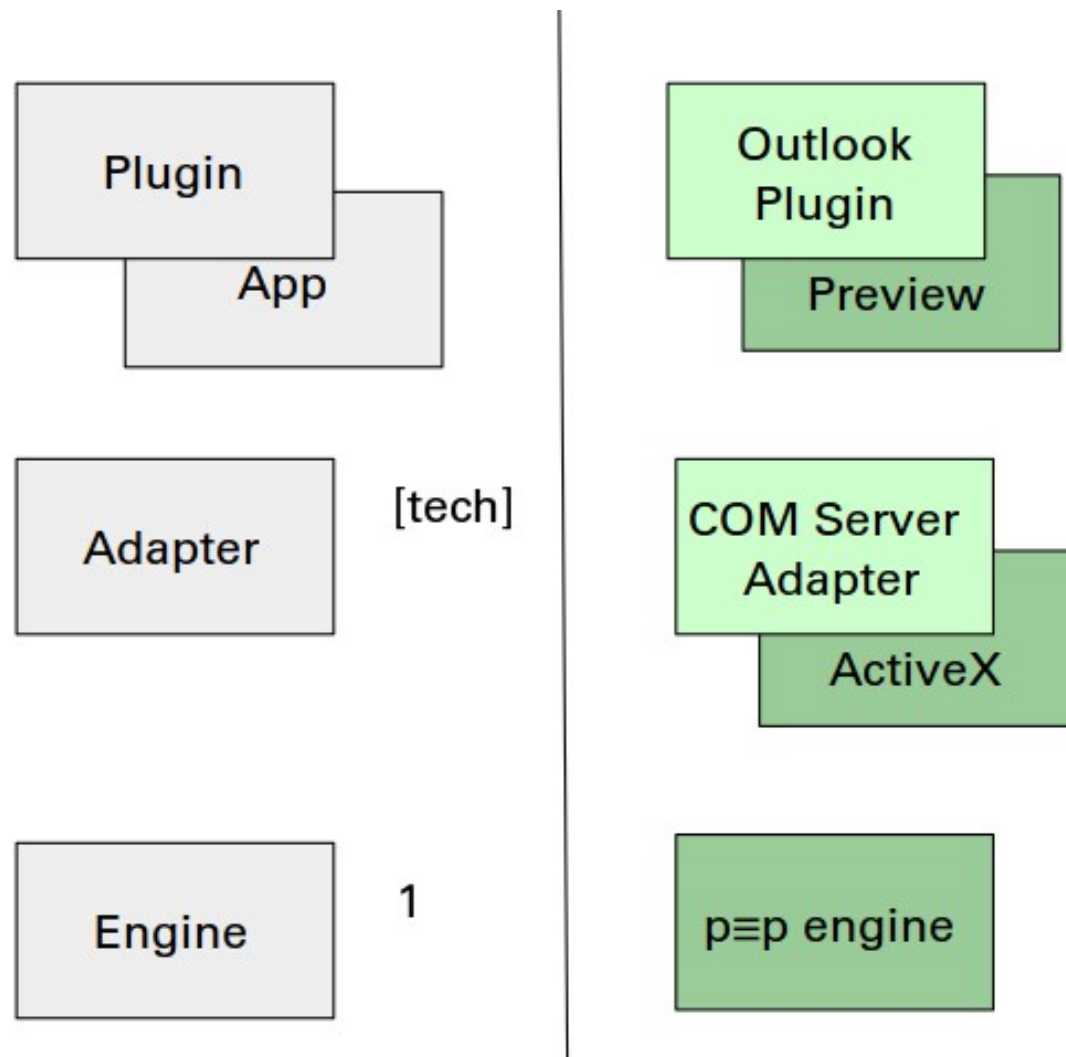
3.2. List of Adapters and Repos

3.3. List of Developing Platforms

3.4. Engine



3.0. p≡p Tech: Architecture



Applications

Adapters

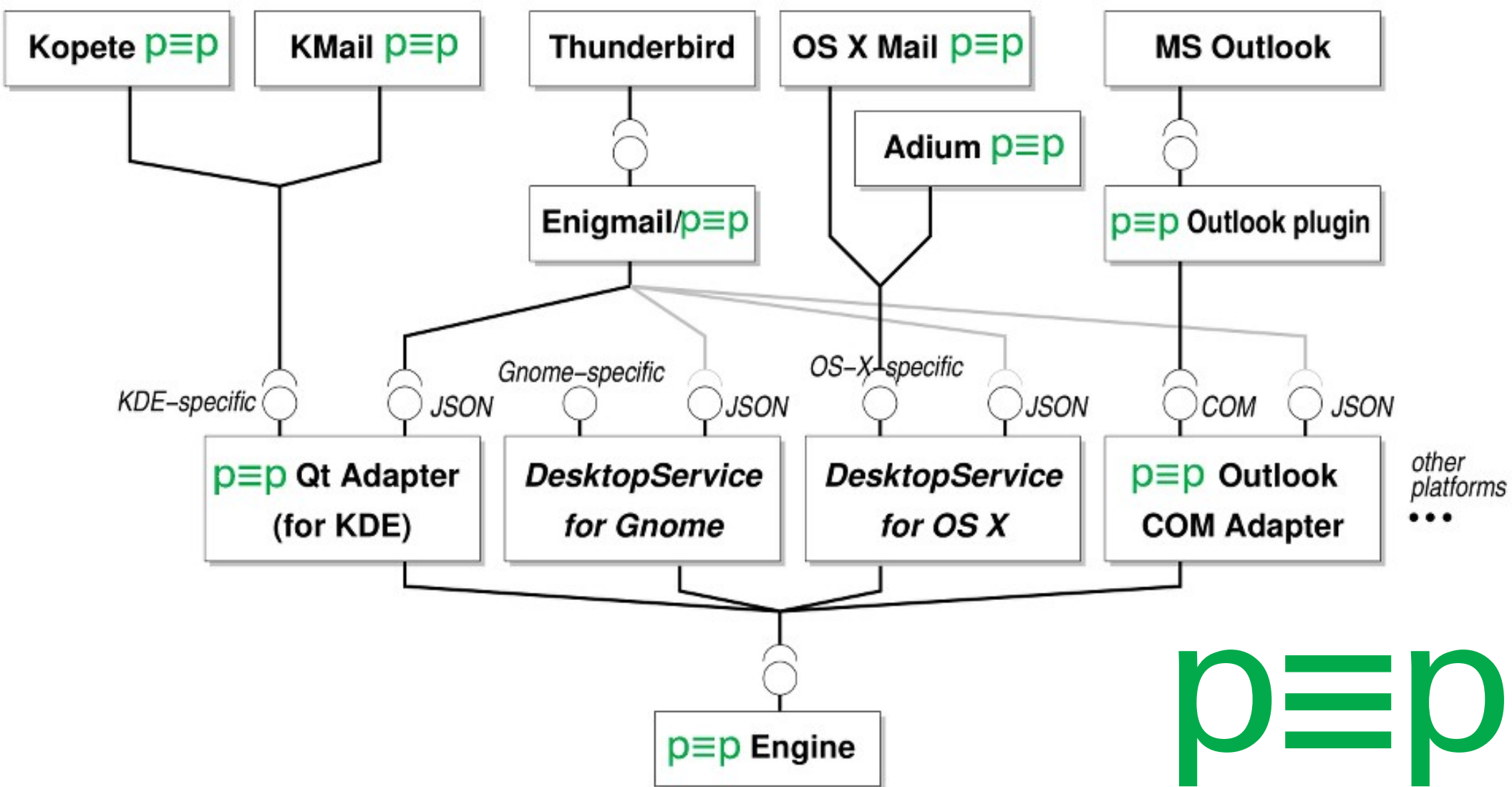
and Engine

p≡p

<https://cacert.pep.foundation/trac>
<https://letsencrypt.pep.foundation/trac>

3.1. p≡p Tech: Engine and Adapters

p≡p on Desktop Operating Systems



3.2. p≡p Tech: Adapters & Repos

MailModel	modelling Message and Folder
netpgp-et	fork of netpgp (iOS adoptions and fixes)
pEpCOMServerAdapter	p≡p COM server adapter
pEpEngine	p≡p engine
pEpJNIAdapter	p≡p JNI adapter
pEpJSONServerAdapter	p≡p JSON adapter
pEpMIME	p≡p MIME library
pEpPythonAdapter	p≡p Python adapter
pEpQtAdapter	p≡p Qt adapter
pEpiOSAdapter	p≡p iOS adapter
pantomime-iOS	fork of pantomime (iOS adoptions)
yml2	>b's YML 2

<https://cacert.pep.foundation/dev>

<https://letsencrypt.pep.foundation/dev>



3.3. p≡p Tech: Developing Platforms

Platforms we are developing on:

iOS

Android

Linux

BSD

MacOS

Windows



3.4. p≡p Tech: Engine

p≡p engine modules

Send-/
Receive

Message
Loopback

Key-
management

Basic API

API

Cryptotech

Message

Transport

implementation

PGP
(GnuPG)
(NetPGP)

OTR

GNUnet

Auto-
transport

email

MIME

XMPP

low-level

NetPGP
fork

Libetpan
fork

p≡p

4 – Applications: Overview

4.0. Current Implementation

4.1. Android via K-9-Fork

4.2. MS Outlook via Add-in

4.3. Thunderbird via Enigmail/p≡p

4.4. Coming soon...



4.0. p≡p Apps: Implementation

Handles OpenPGP and S/MIME
without any hassle for the user:

Automatically encrypts

Encrypts the subject inline

No key management needed

No keyserver or other centralized infrastructure

Fingerprints \equiv Trustwords

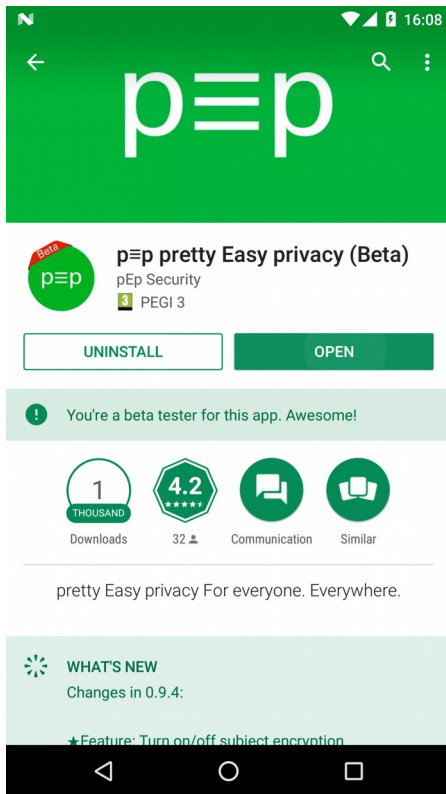
Opt-in passphrase for keys

Header encrypted and obfuscated

p≡pSync

p≡p

4.1. p≡p Apps: Android/K-9-Fork



Ready to use

Available on
Play Store and F-Droid



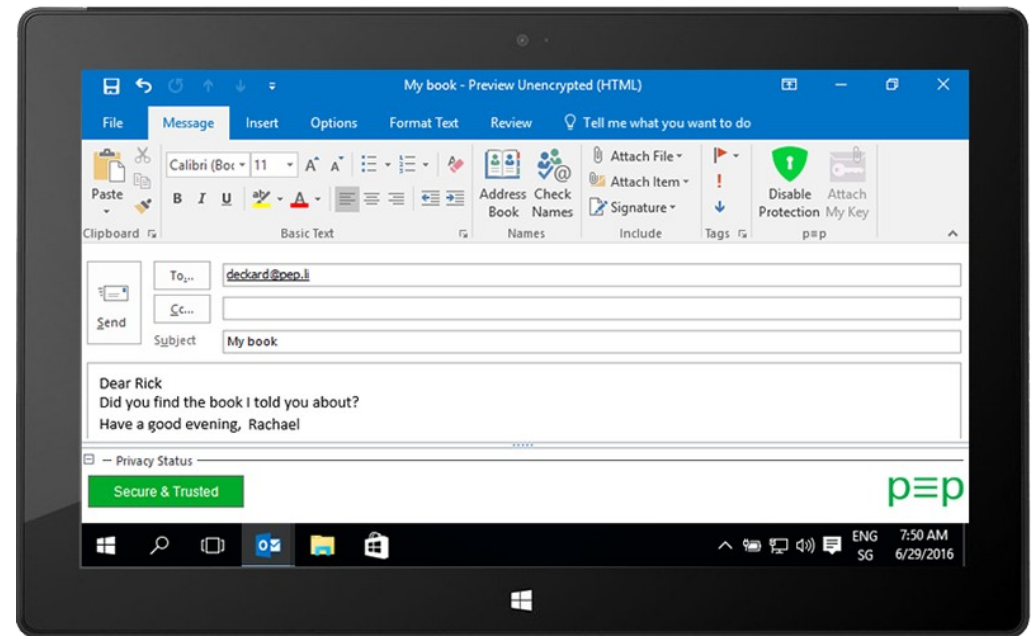
4.2. p≡p Apps: Windows/Outlook

Ready to use

Available on
prettyeasyprivacy.com

Free as in freedom
not as in free beer.

(Contact us for testing license)



p≡p

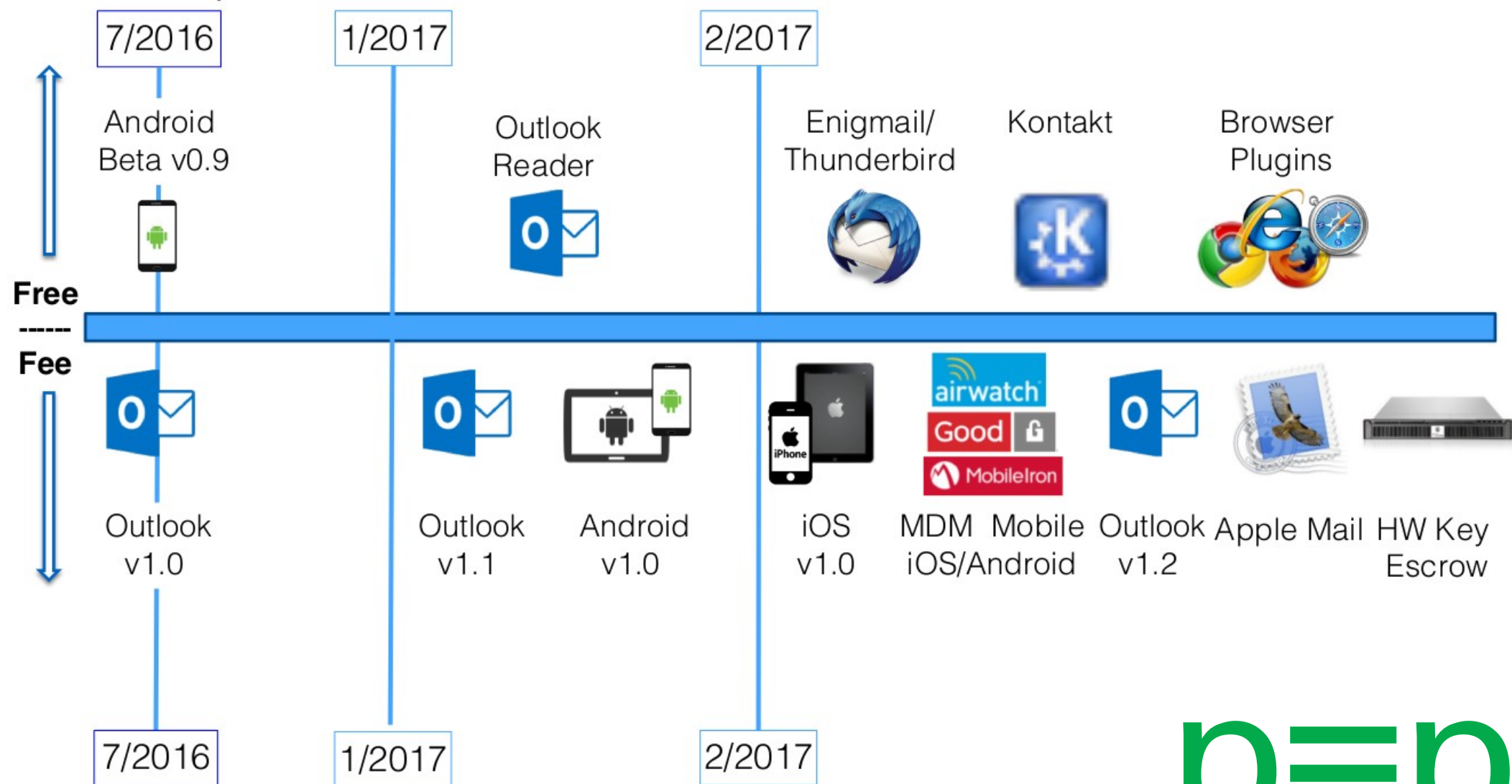
4.3. p≡p Apps: Thunderbird/Enigmail

Coming with
next release of Enigmail

No need for users to manage keys
(but “advanced/expert” mode still available)



4.4. p≡p Apps: Coming...



p≡p

5 – Applications: Demos: Overview

5.0. Intro

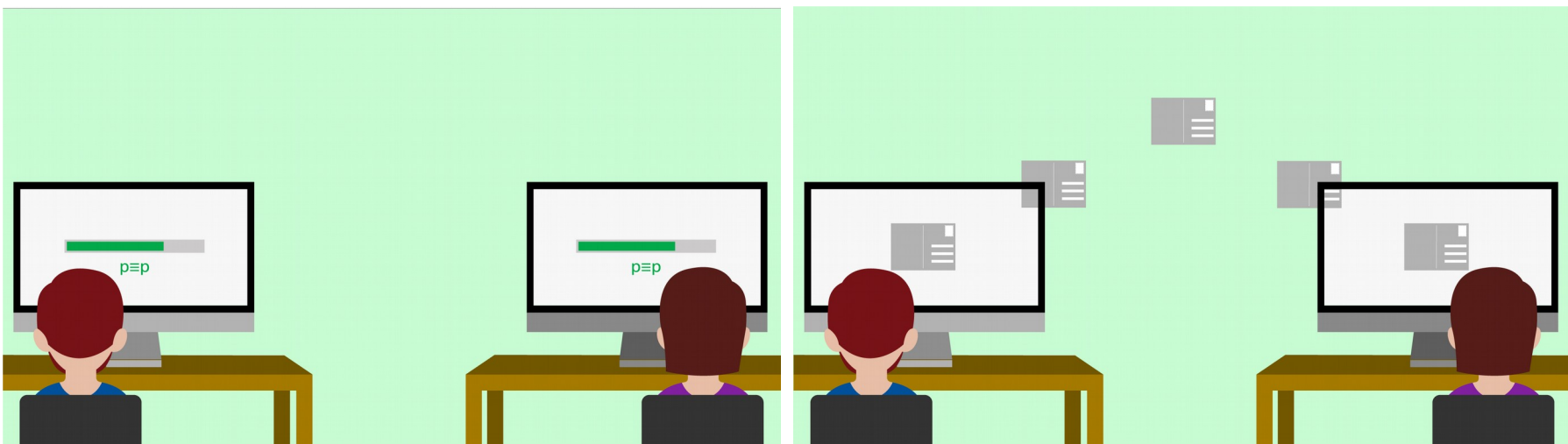
5.1. Android

5.2. MS Outlook

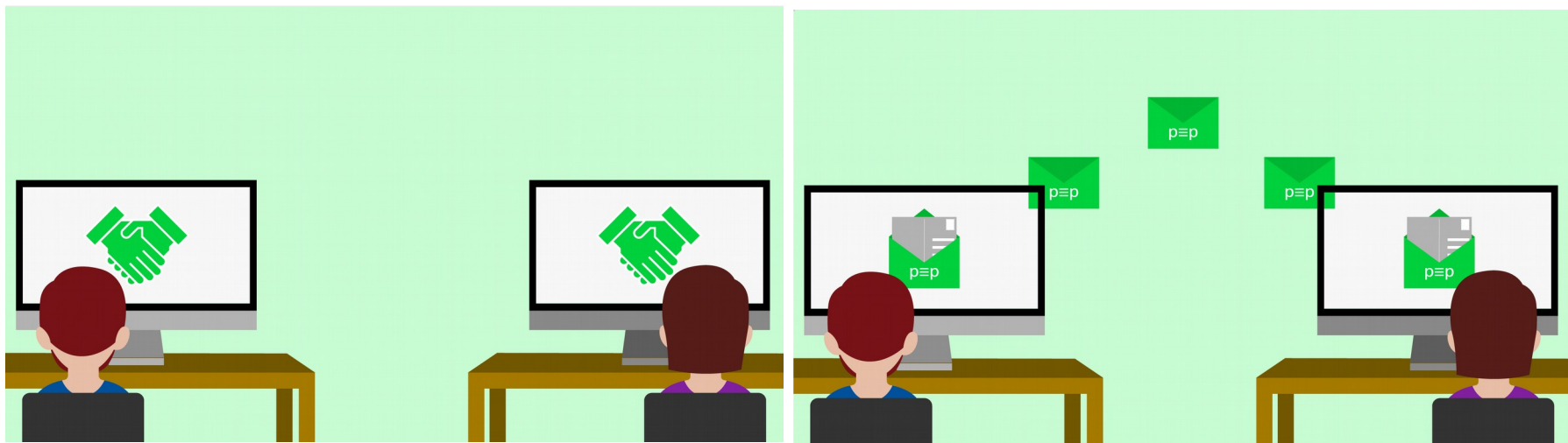
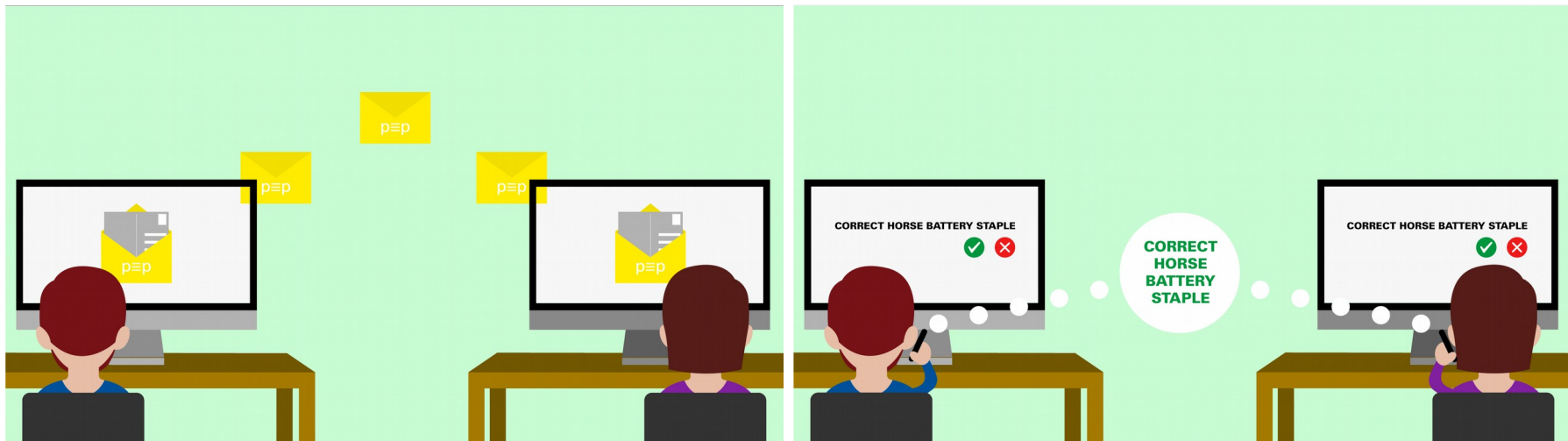
p≡p

p≡p

$p \equiv p$
Apps



Intro

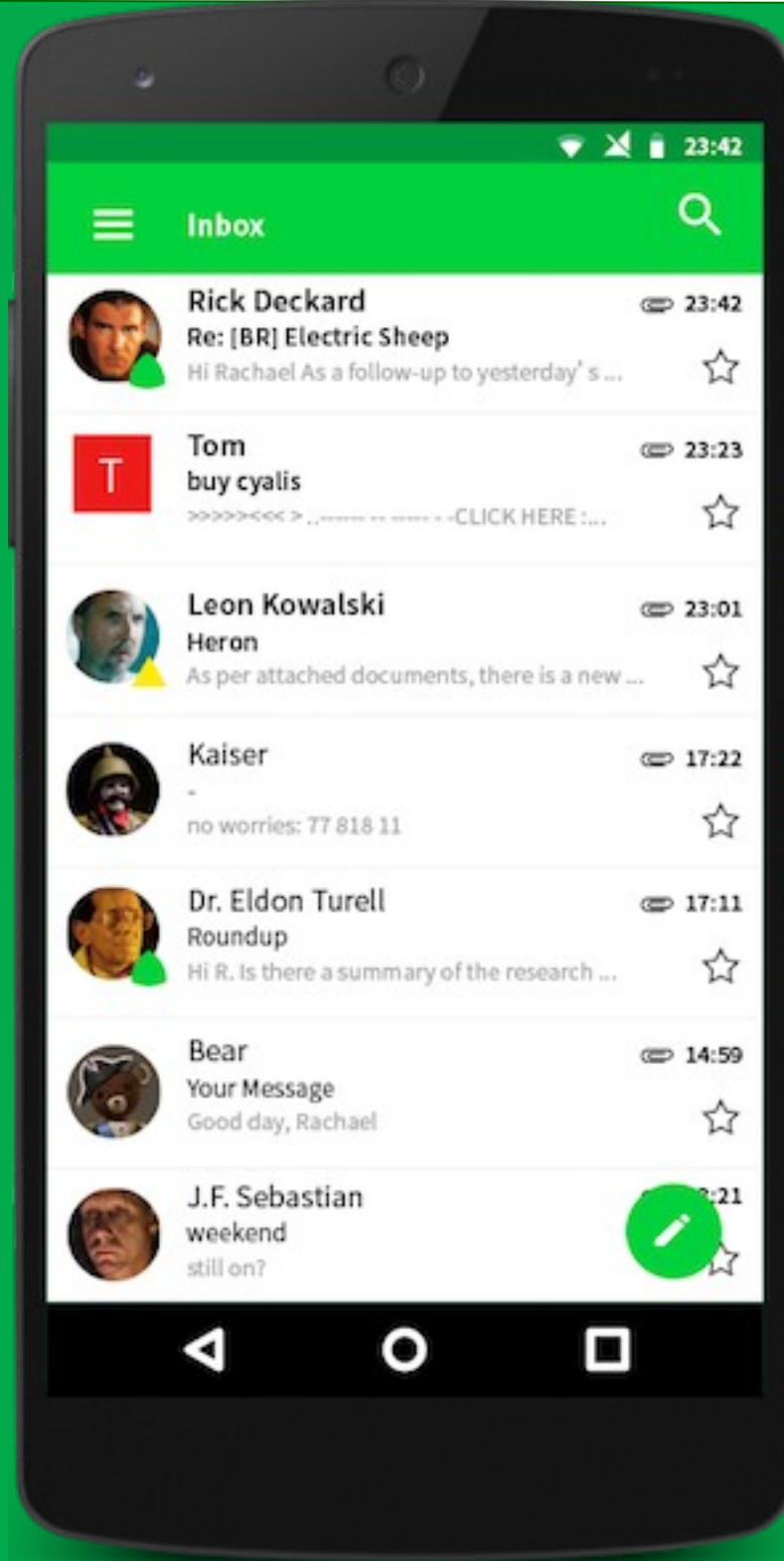


$p \equiv p$
Apps

Intro



p≡p
Apps



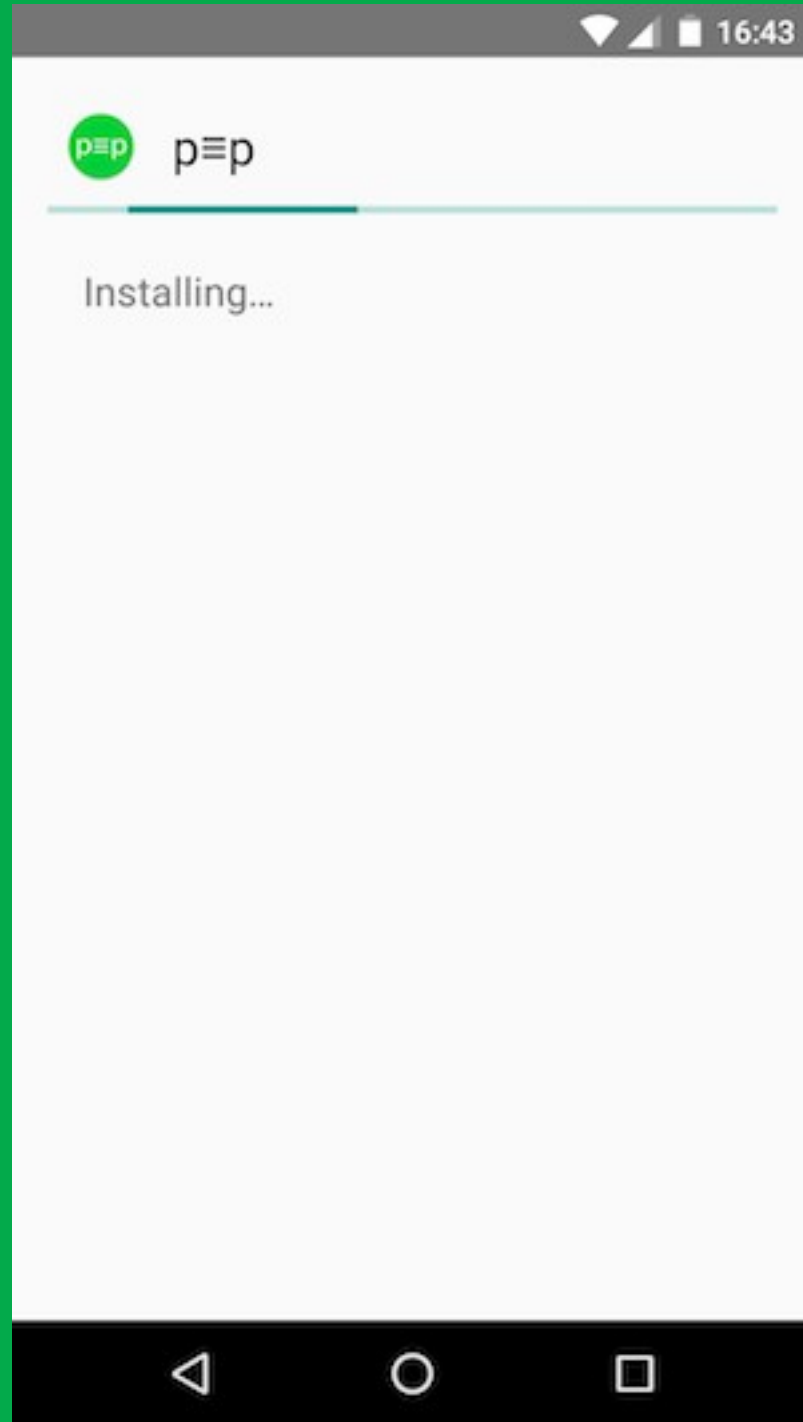
Android

Version 4.3
or higher

Play-Store
or F-Droid

p≡p

p≡p
Apps

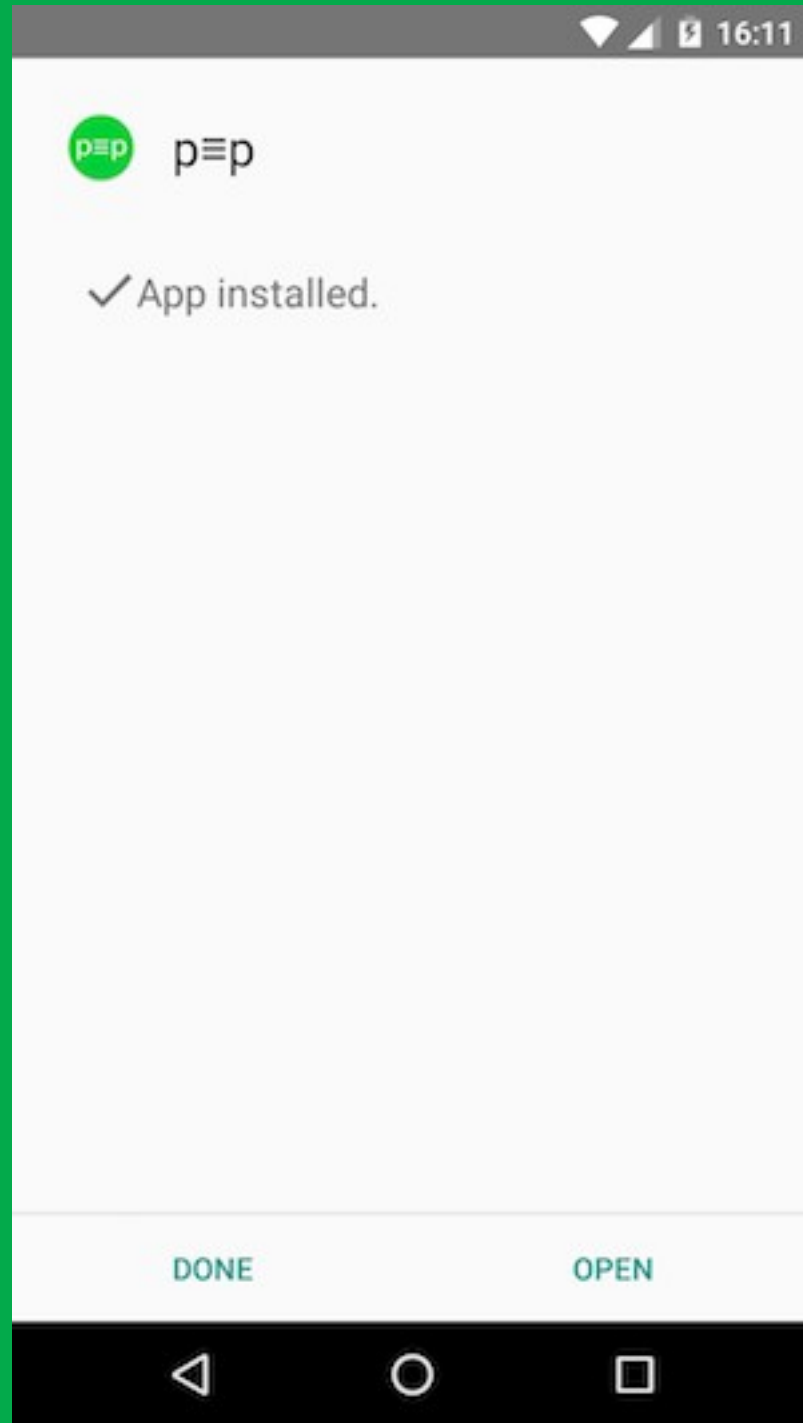


Android

Installing

p≡p

p≡p
Apps

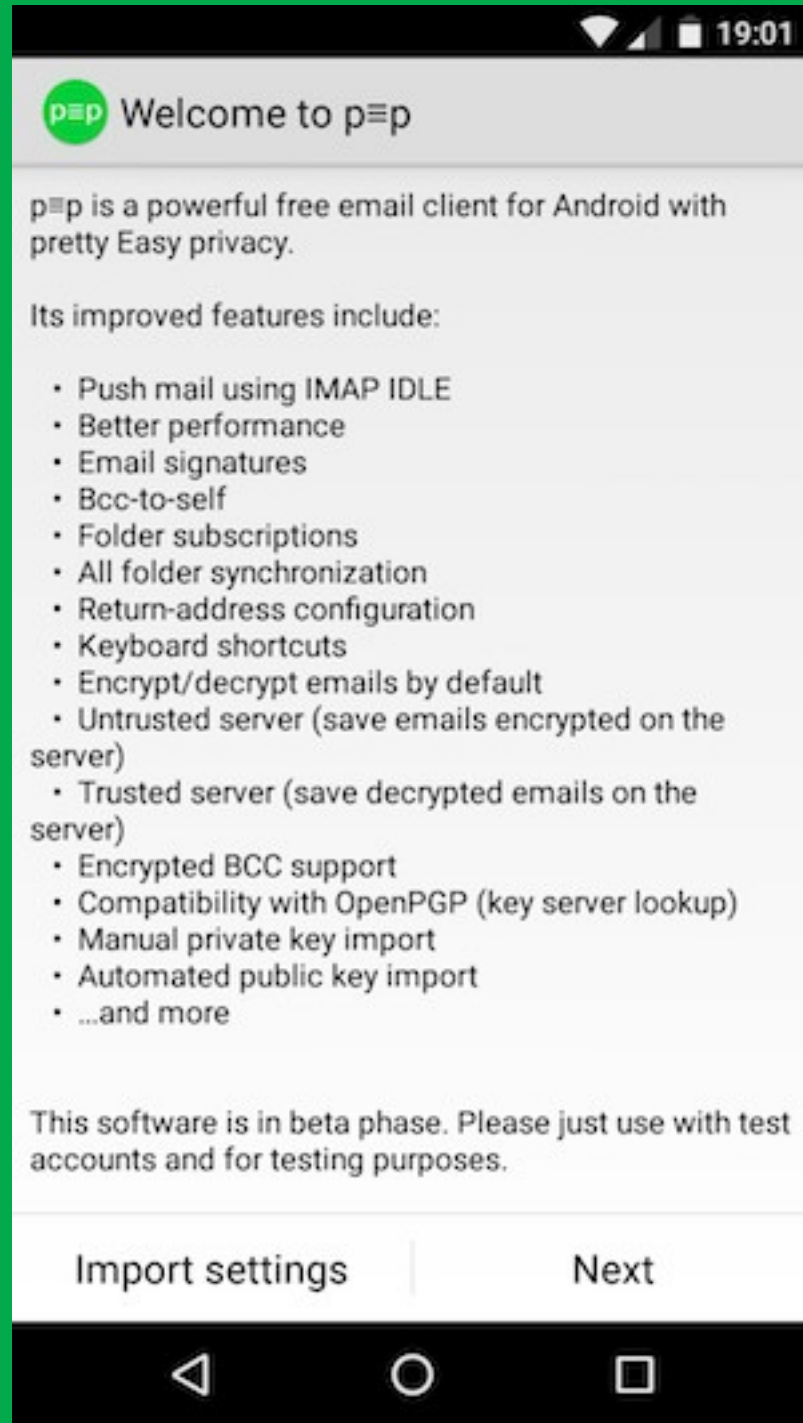


Android

Installed

p≡p

p≡p Apps

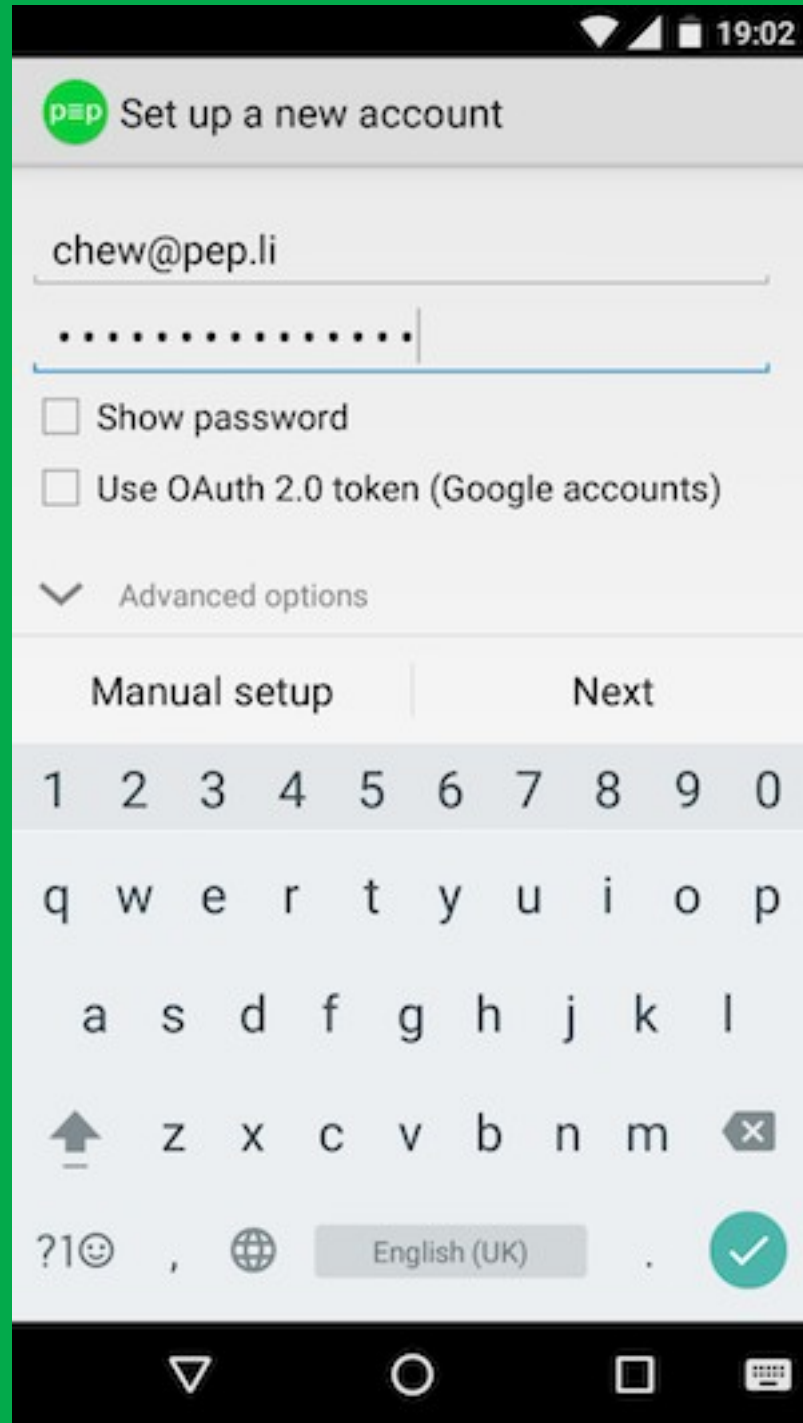


Android

Welcome screen after fresh install

p≡p

p≡p
Apps



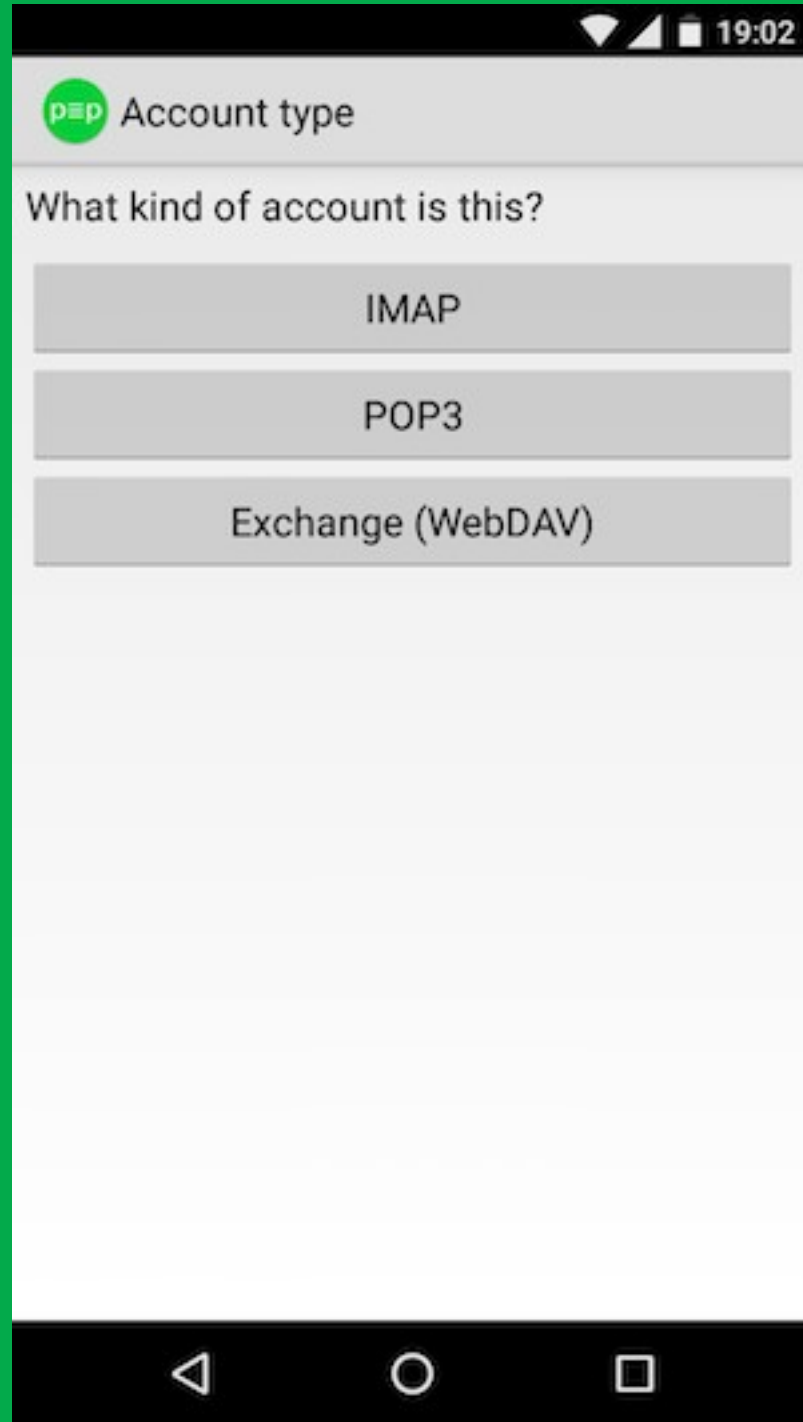
Android

Setup new account

(keys will be generated automatically. For importing existing keys you'll need a workaround till version with pEpSync is ready)

p≡p

p≡p
Apps



Android

Setup
account type
(we'll choose
IMAP here)

p≡p

p≡p
Apps

The screenshot shows the 'Incoming server settings' screen of the p≡p email client. The settings are as follows:

- IMAP server: imap.pep.li
- Security: SSL/TLS
- Port: 993
- Username: chew@pep.li
- Authentication: Normal password
- Password:
- ☒ Auto-detect IMAP namespace
- IMAP path prefix:
- Use compression on network:

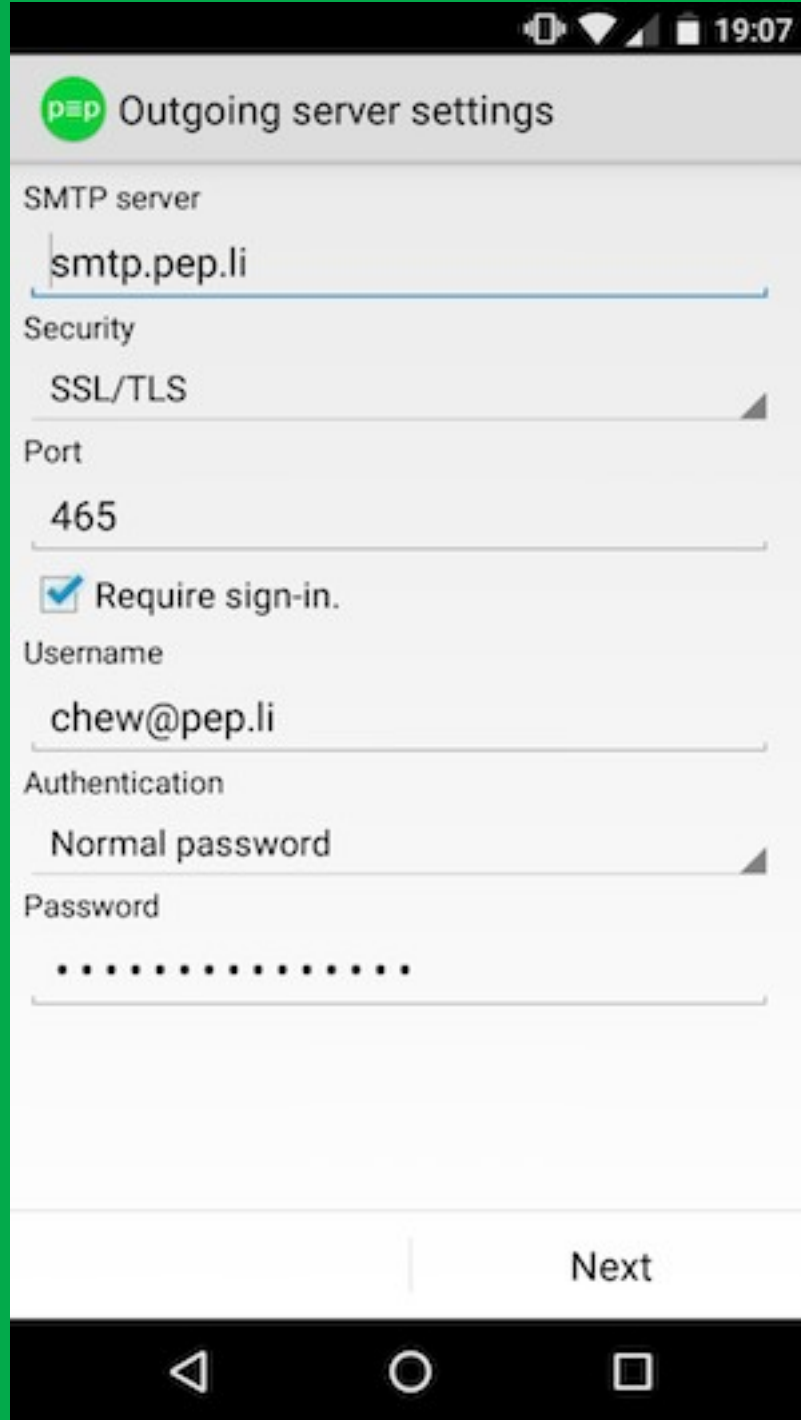
At the bottom right, there is a 'Next' button. The Android navigation bar is visible at the very bottom.

Android

IMAP server
settings

p≡p

p≡p
Apps



The screenshot shows the 'Outgoing server settings' screen for the p≡p app. The status bar at the top indicates the time is 19:07. The settings are as follows:

- SMTP server:** smtp.pep.li
- Security:** SSL/TLS
- Port:** 465
- Require sign-in:** ☒
- Username:** chew@pep.li
- Authentication:** Normal password
- Password:** (masked with dots)

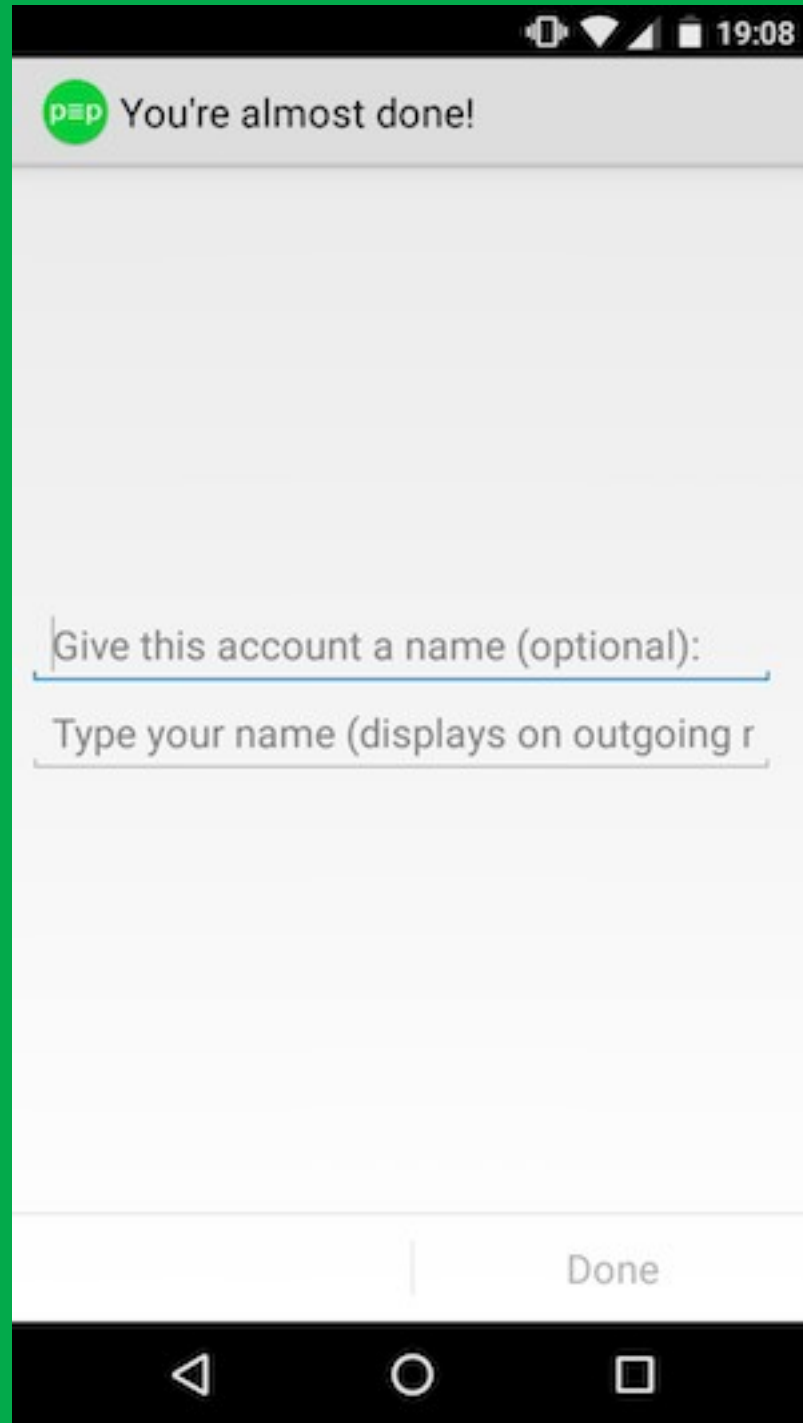
A 'Next' button is located at the bottom right of the settings form. The Android navigation bar is visible at the very bottom.

Android

SMTP server
settings

p≡p

p≡p
Apps

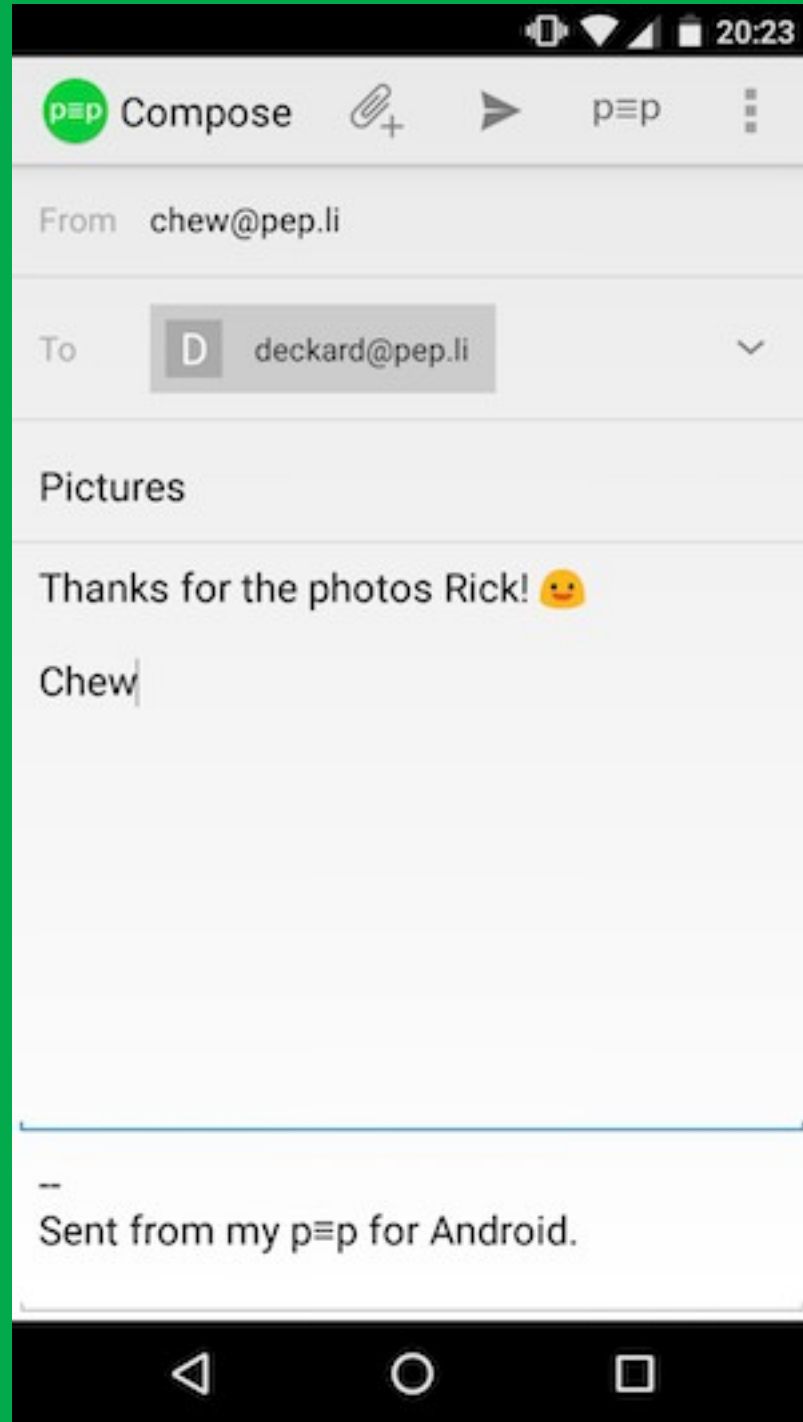


Android

Setup
account
name

p≡p

p≡p
Apps



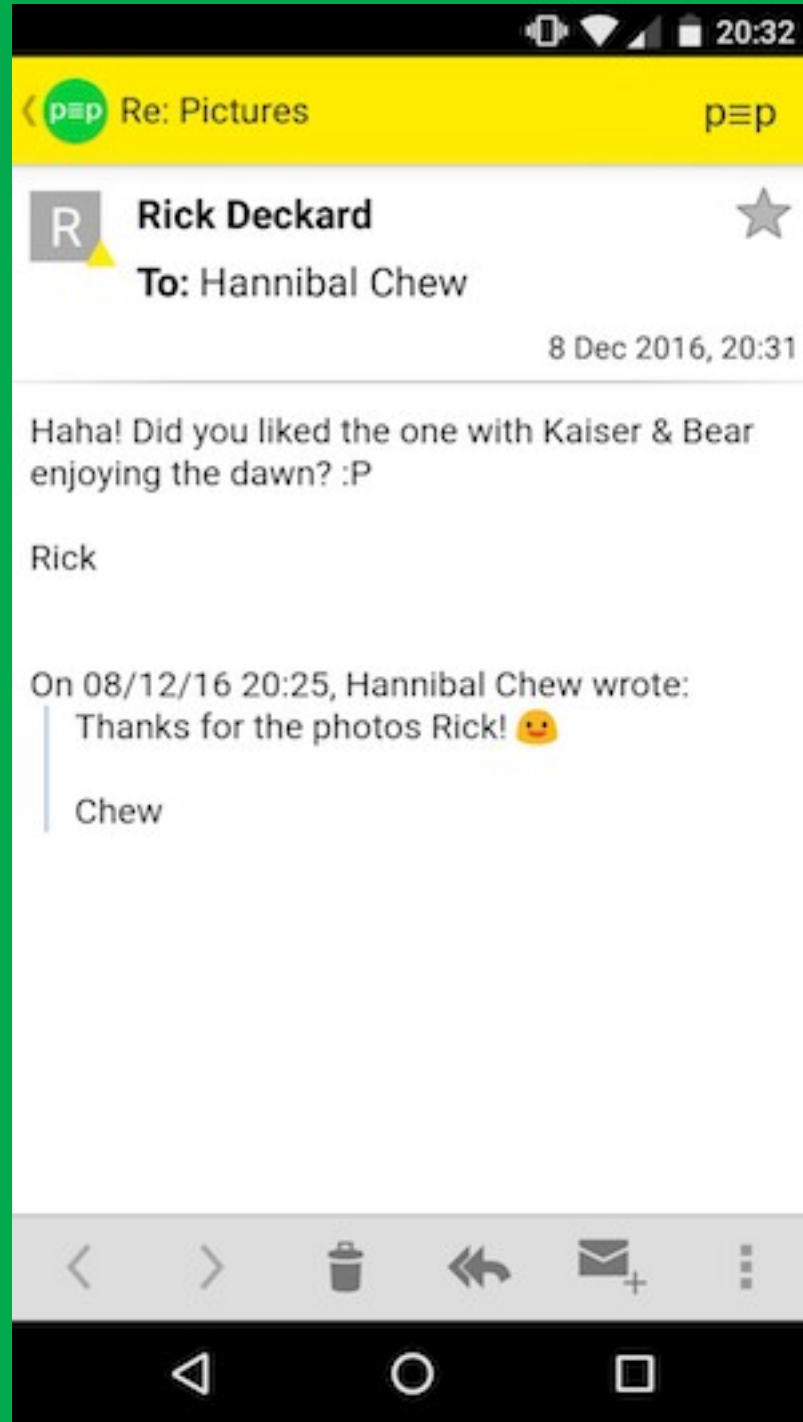
Android

Compose
view

Grey mode:
unencrypted
plain text, key
will be attached

p≡p

p≡p
Apps

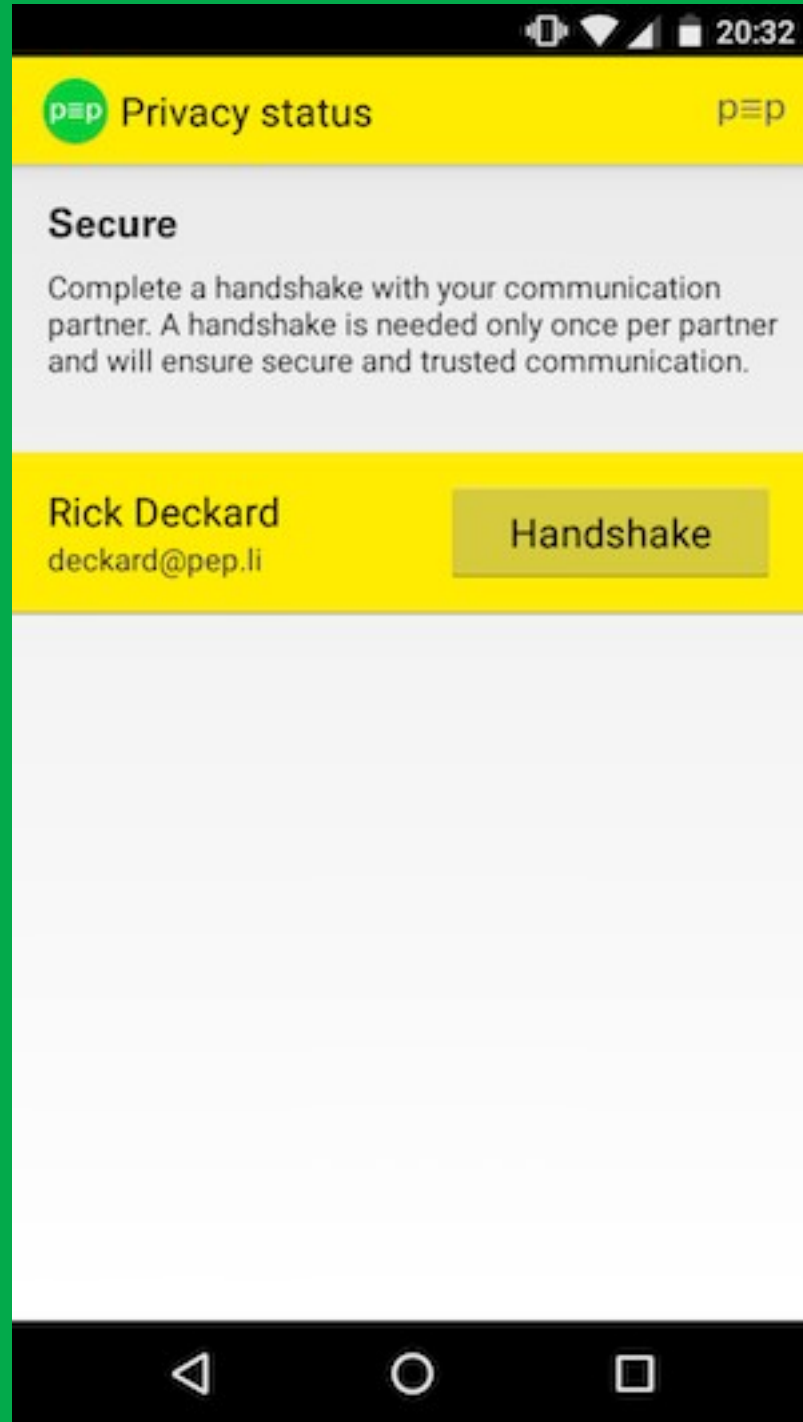


Android

Got reply with
attached key
Yellow mode
Click p≡p in the
upper corner

p≡p

p≡p
Apps

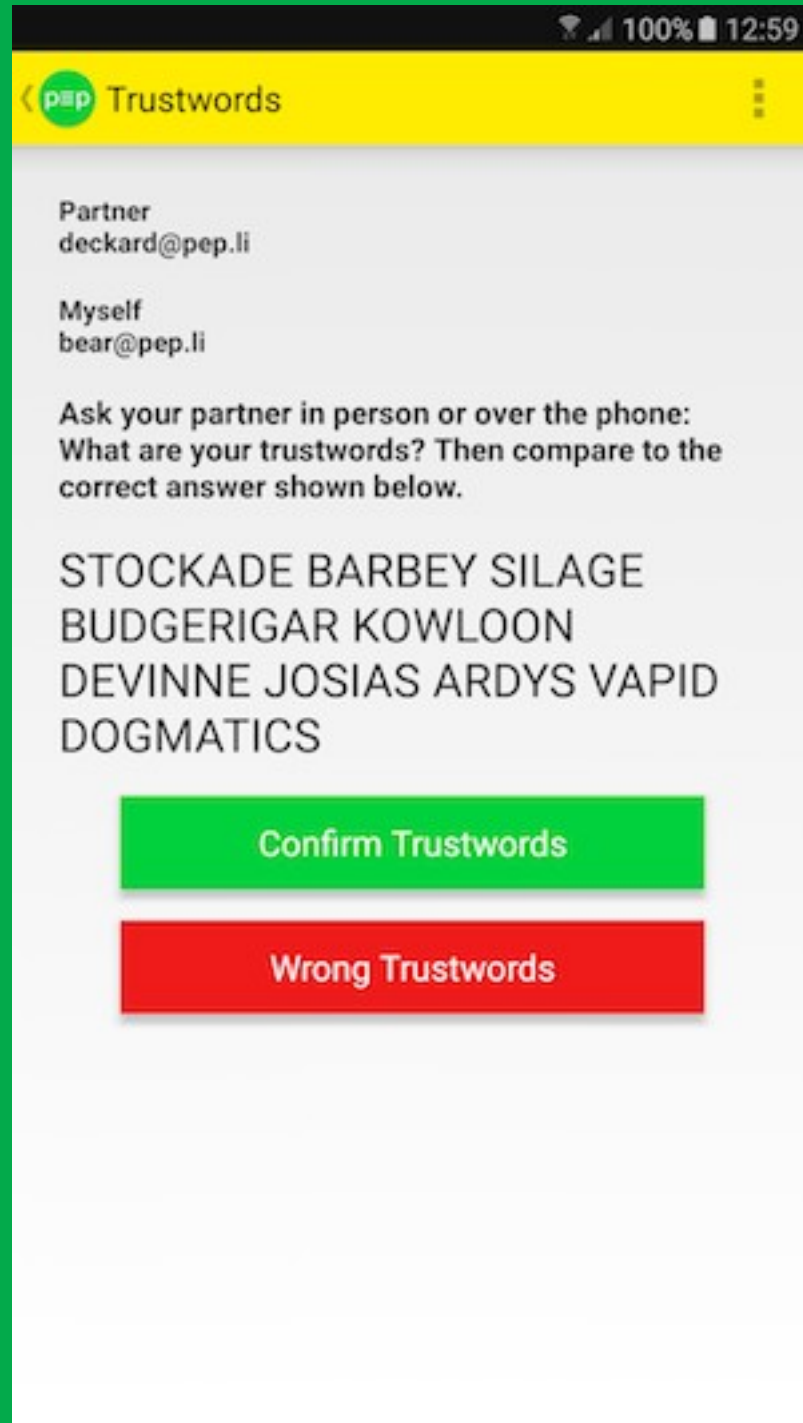


Android

Asking for
handshake

p≡p

p≡p
Apps

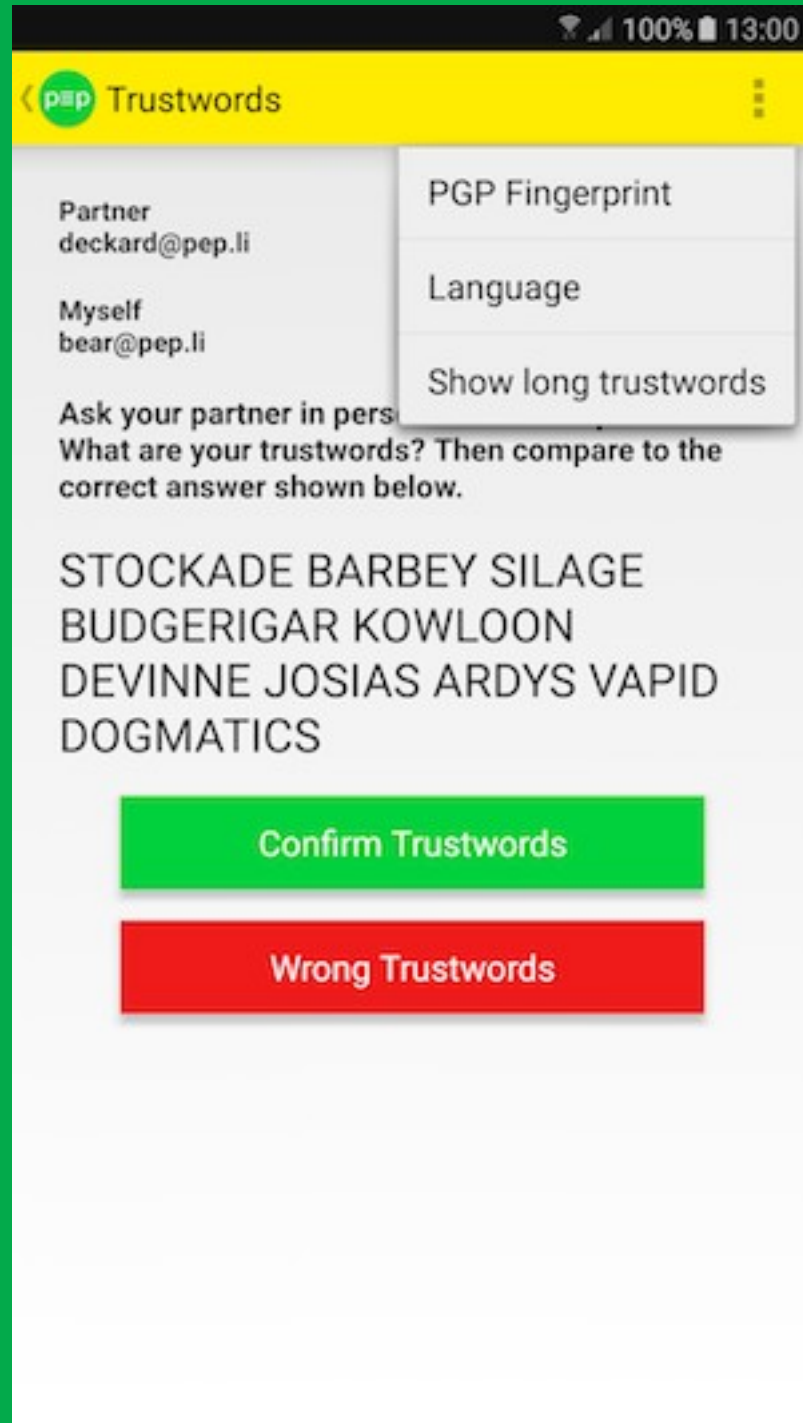


Android

Showing
trustwords

p≡p

p≡p
Apps



Android

Trustword
Menue

p≡p

p≡p
Apps



Android

Trustword
language
selector

p≡p

p≡p
Apps

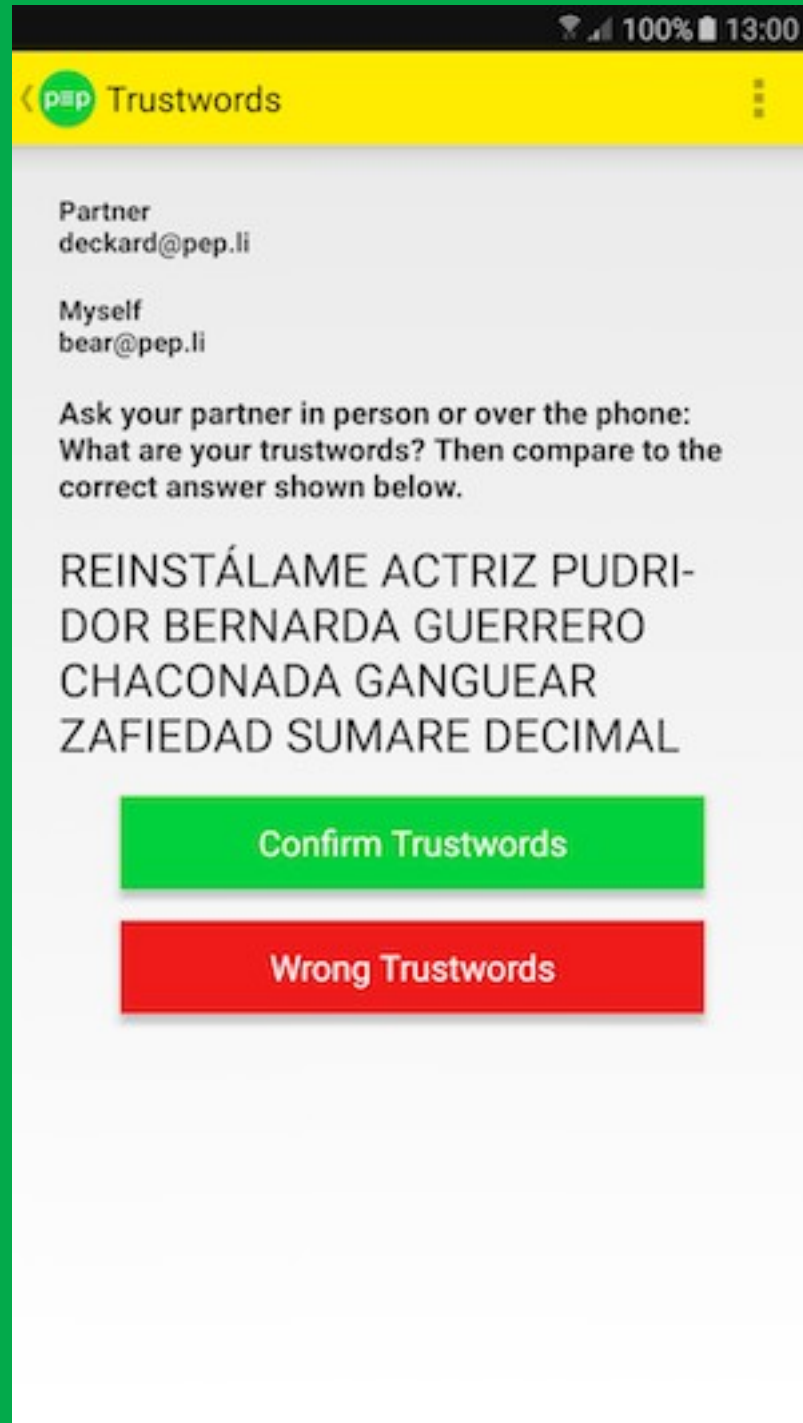


Android

Trustword
language
selector

p≡p

p≡p
Apps

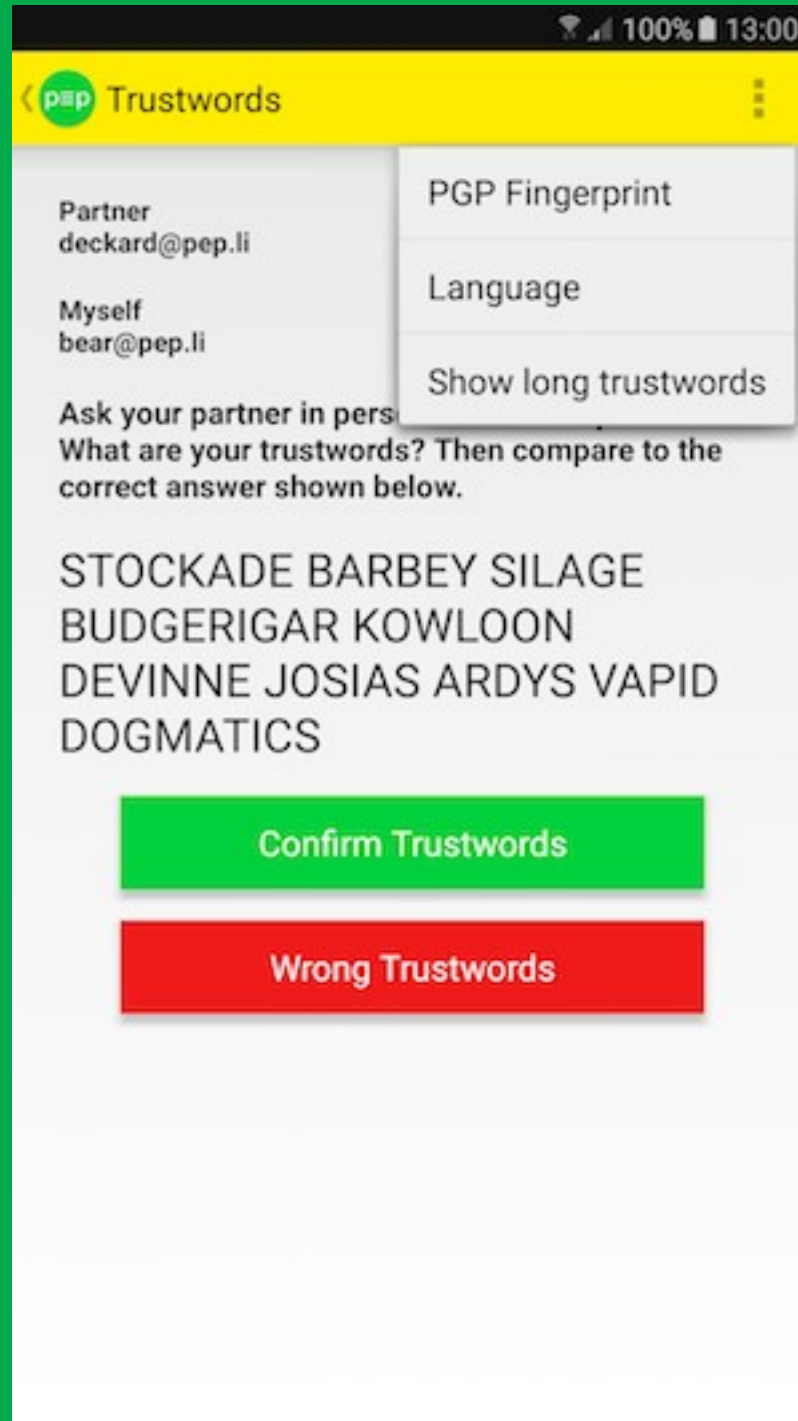


Android

Trustwords
language
selected
spanish

p≡p

p≡p
Apps

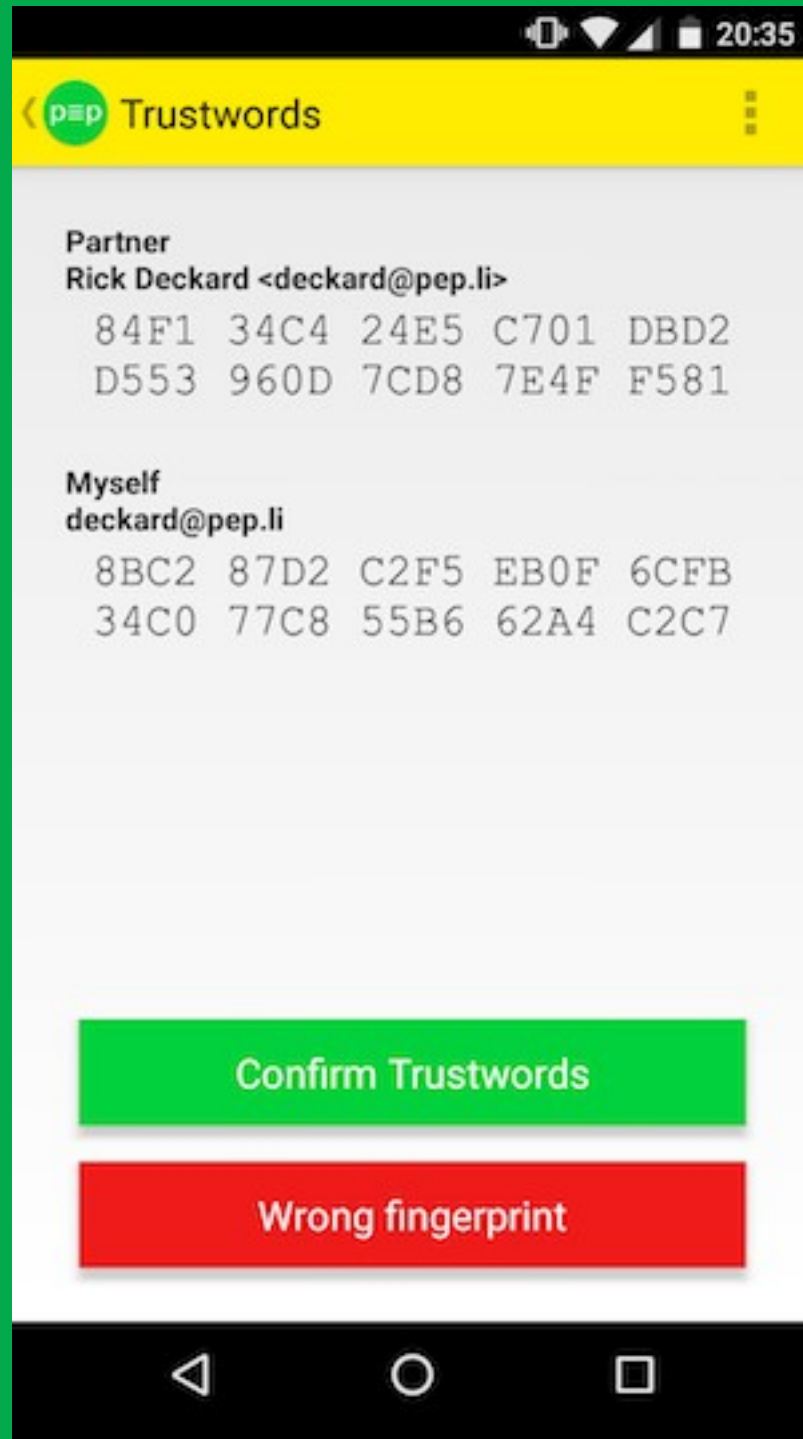


Android

Trustword
Menue

p≡p

p≡p
Apps

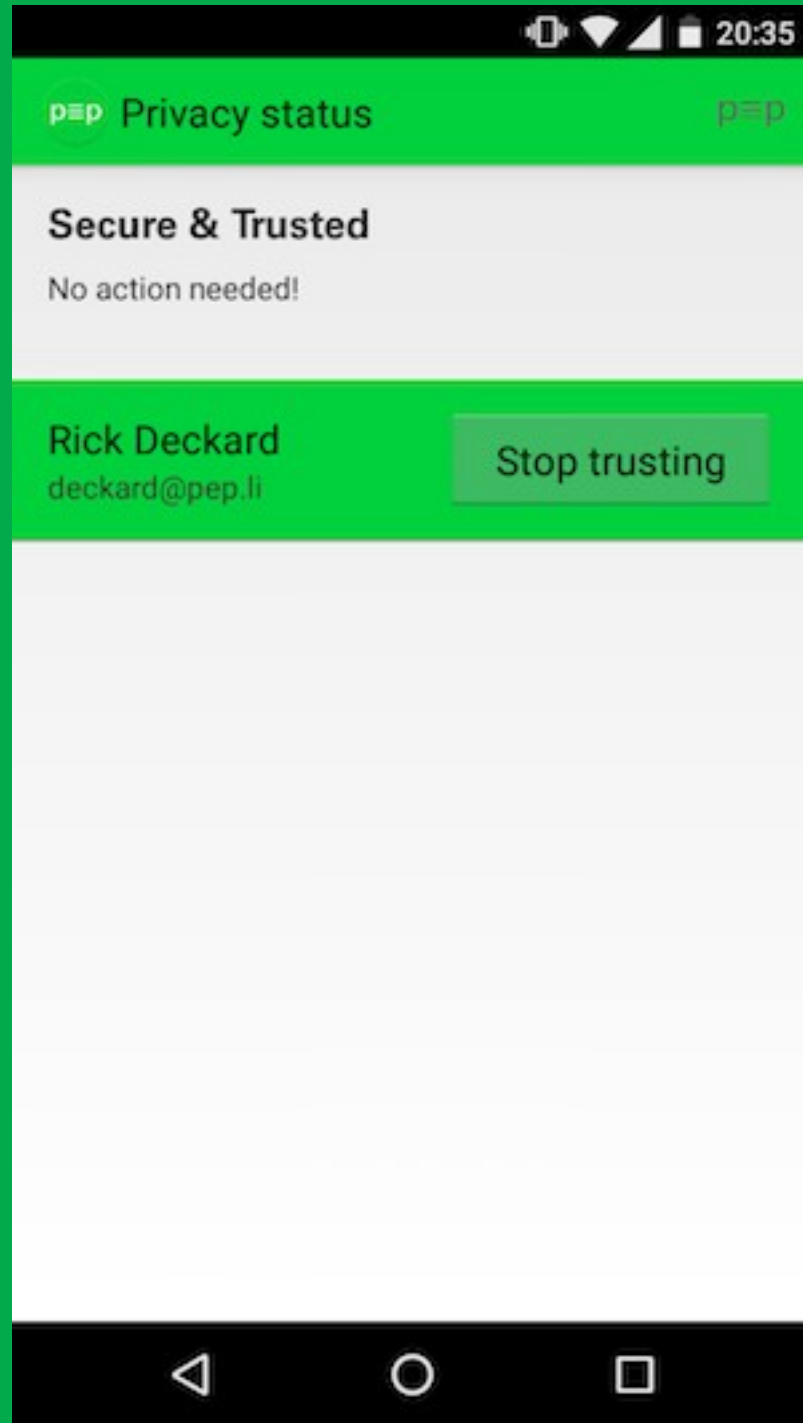


Android

selected
PGP
Fingerprints

p≡p

p≡p
Apps

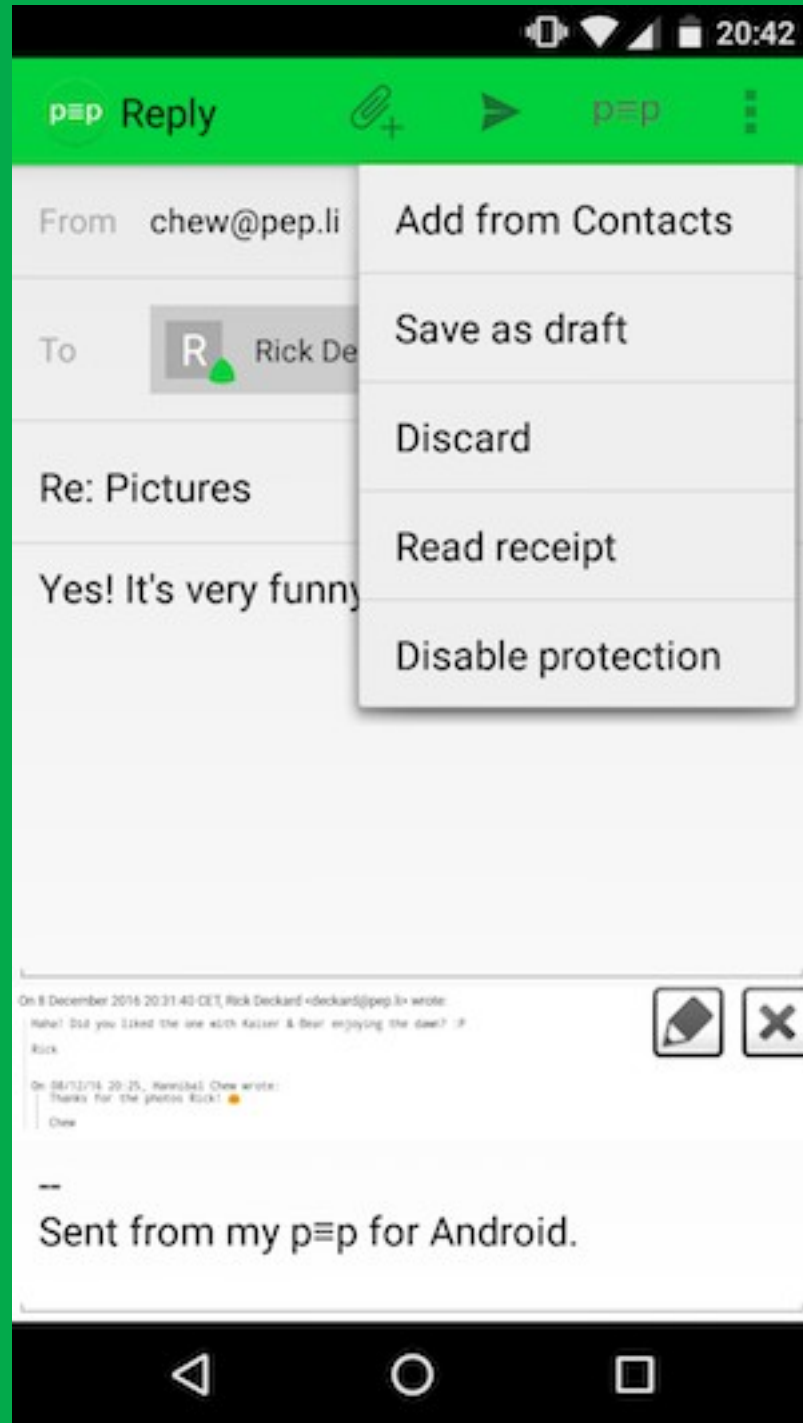


Android

confirmed
Trustwords/
fingerprints:
Green mode

p≡p

p≡p
Apps

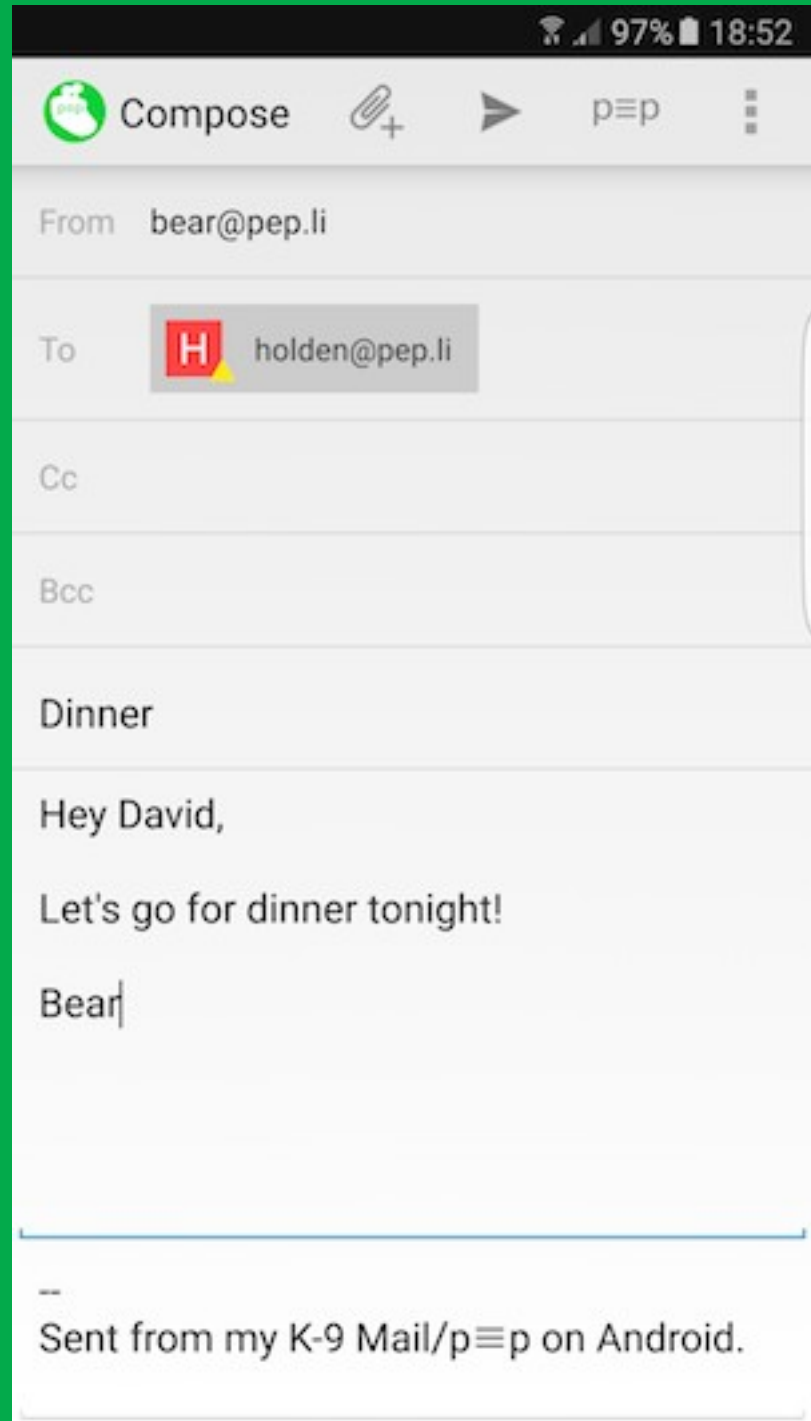


Android

Option:
disable
protection

p≡p

p≡p Apps



Android

Outgoing
mail

disabled
protection,
grey mode

p≡p

p≡p
Apps



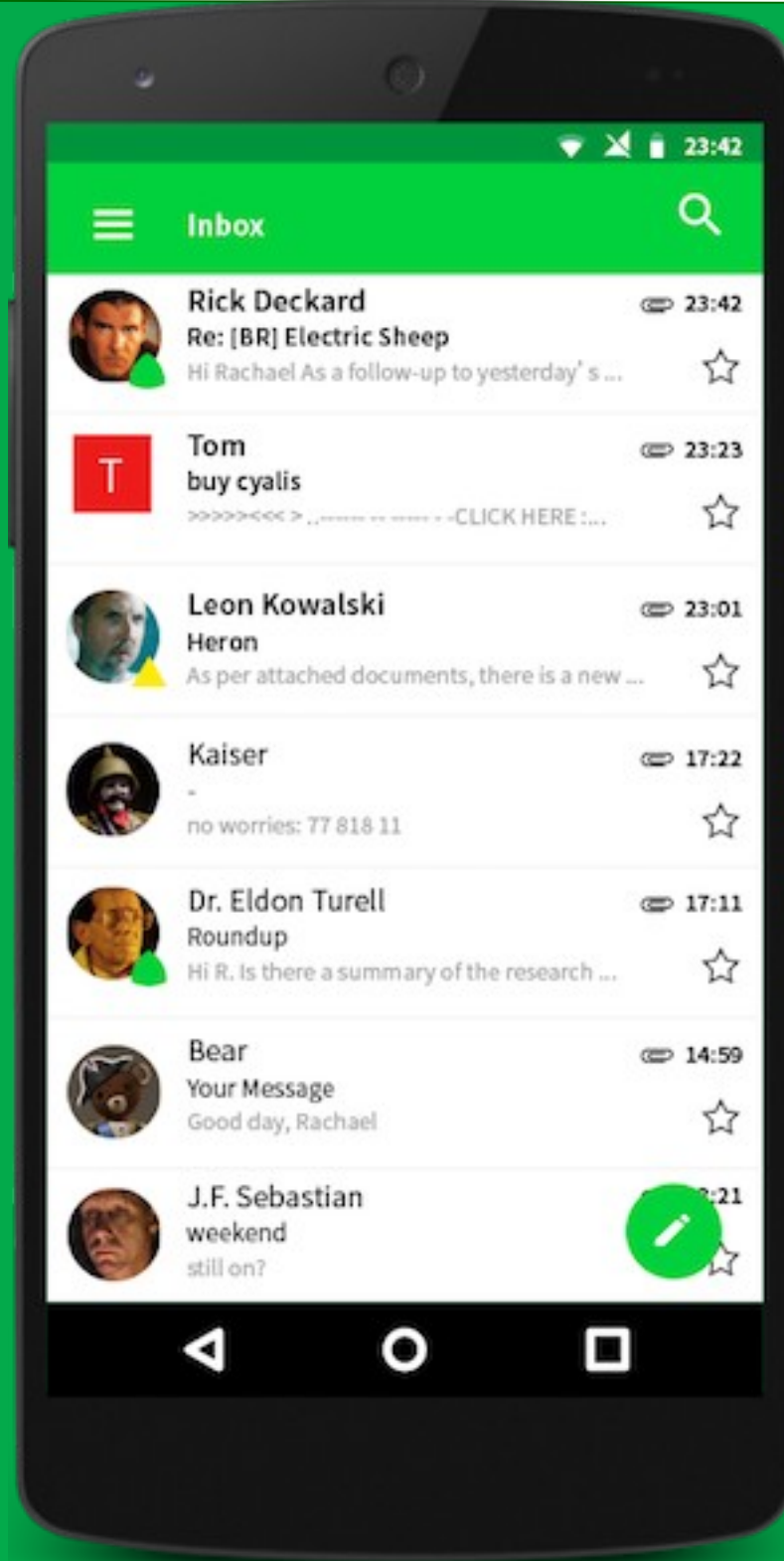
Android

Incoming
mail

disabled
protection,
grey mode

p≡p

p≡p
Apps

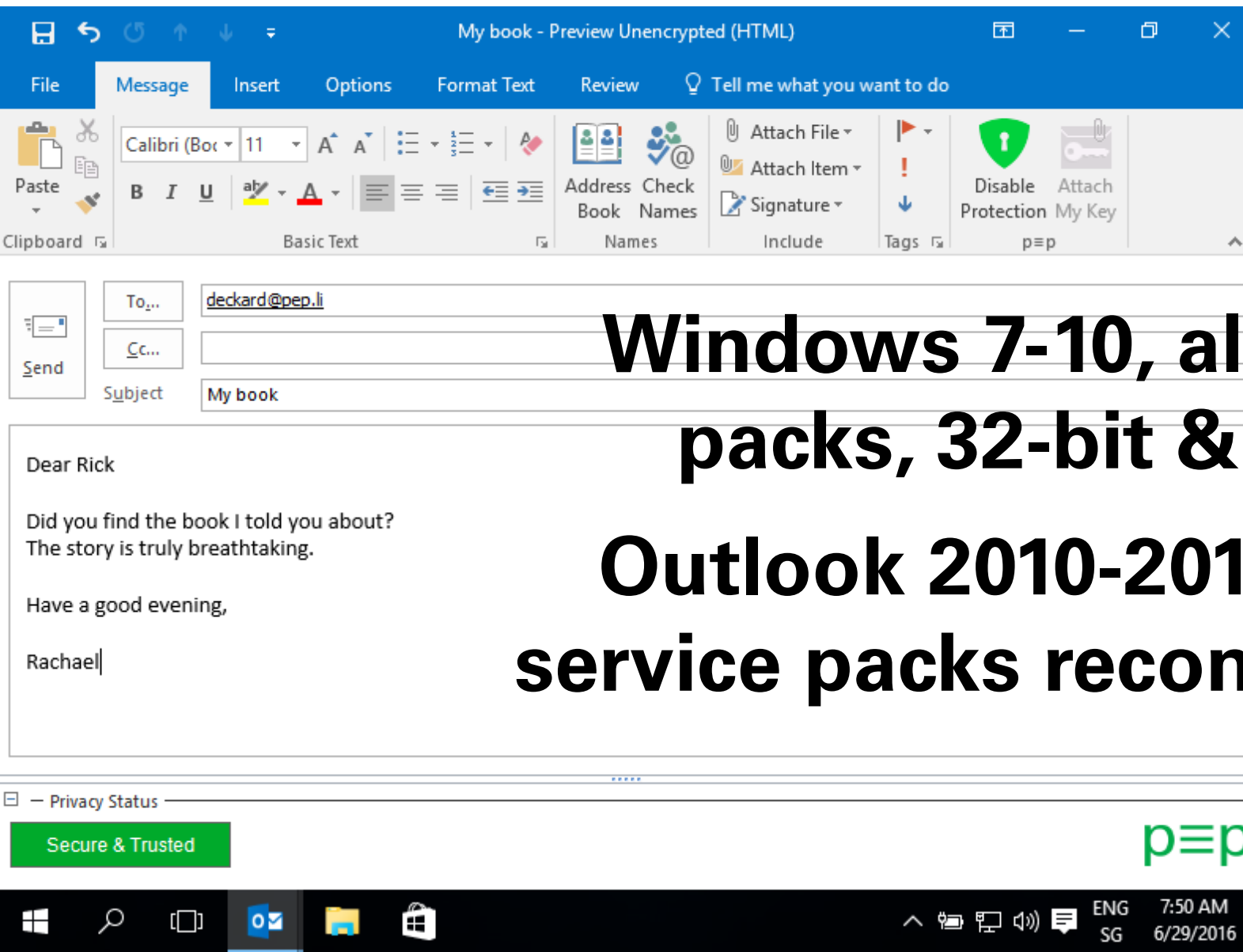


Android

Available on
Play-Store
or F-Droid

p≡p

p≡p Apps: Windows/Outlook

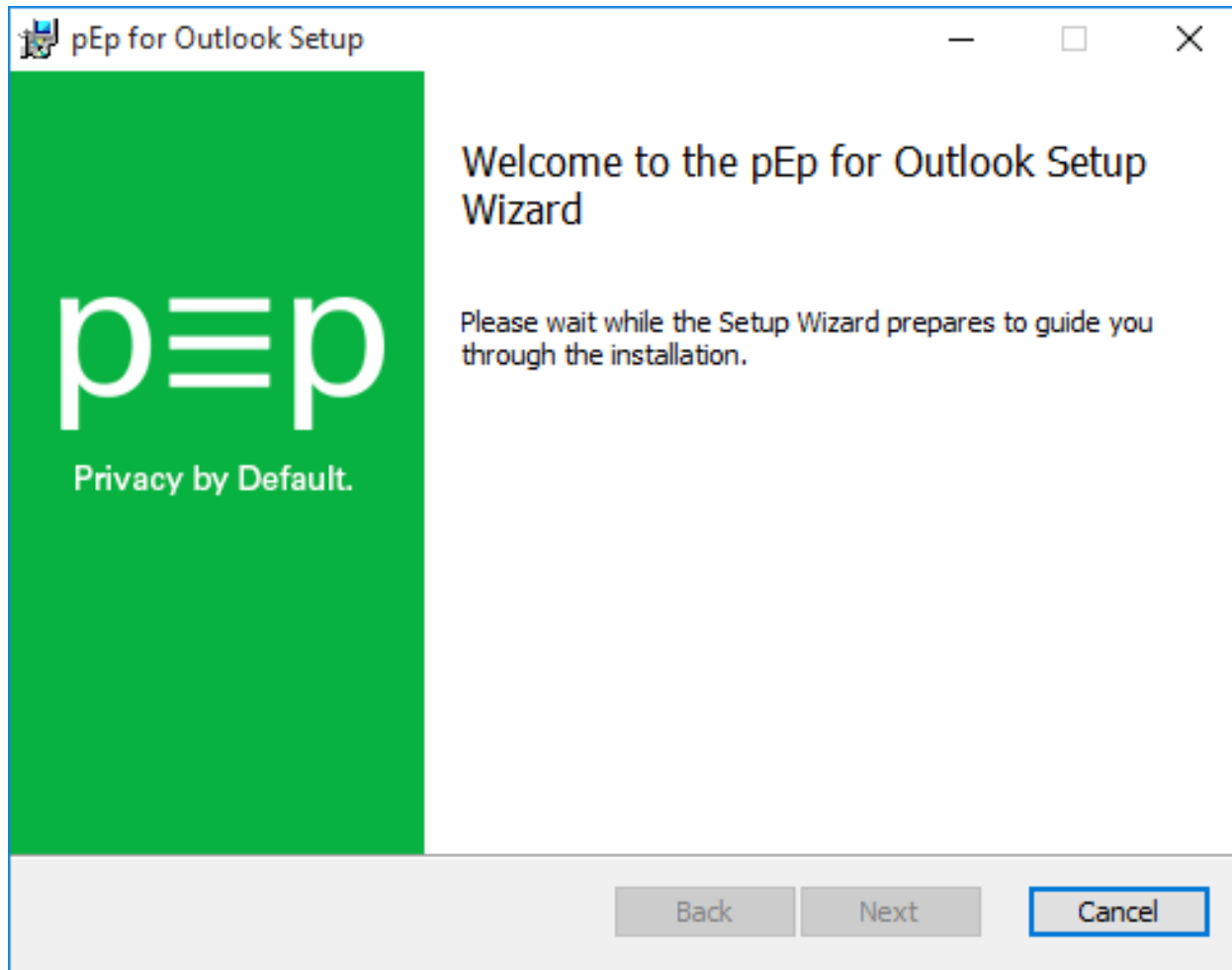


**Windows 7-10, all service
packs, 32-bit & 64-bit
Outlook 2010-2016 (latest
service packs recommended)**

p≡p

p≡p

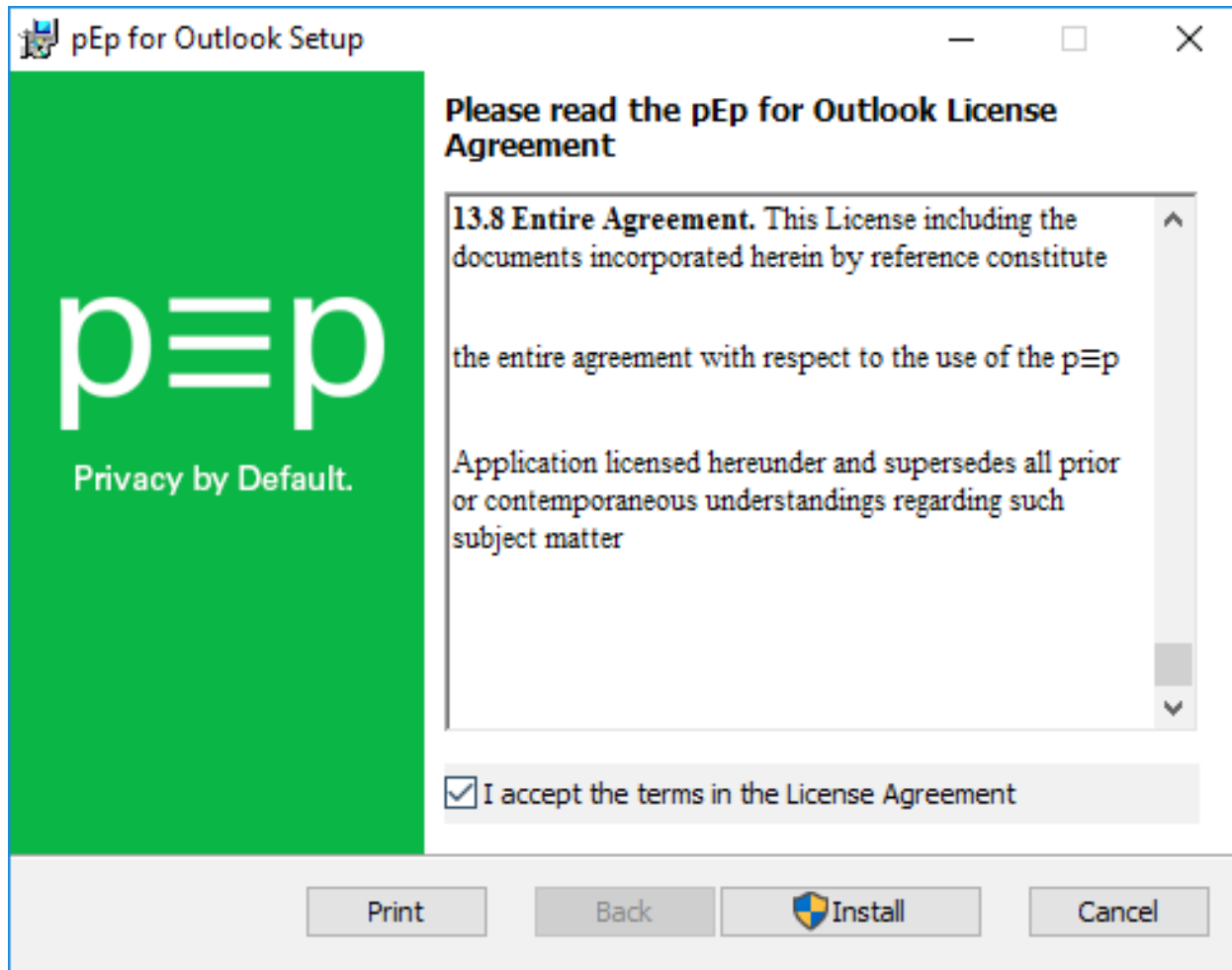
p≡p Apps: Windows/Outlook



Start
installation



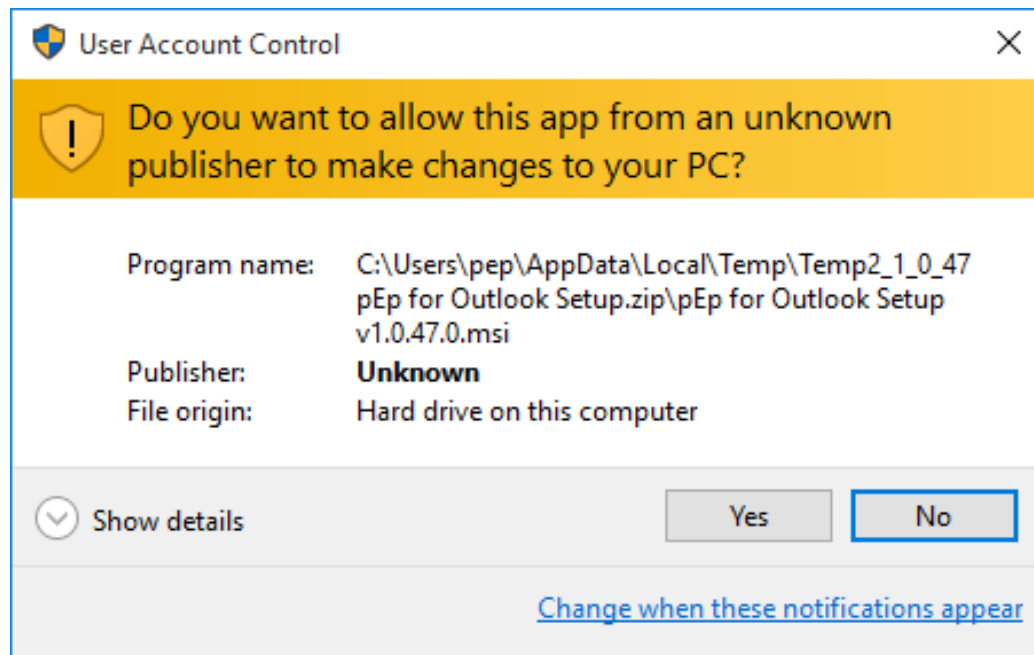
p≡p Apps: Windows/Outlook



Accept license
agreement



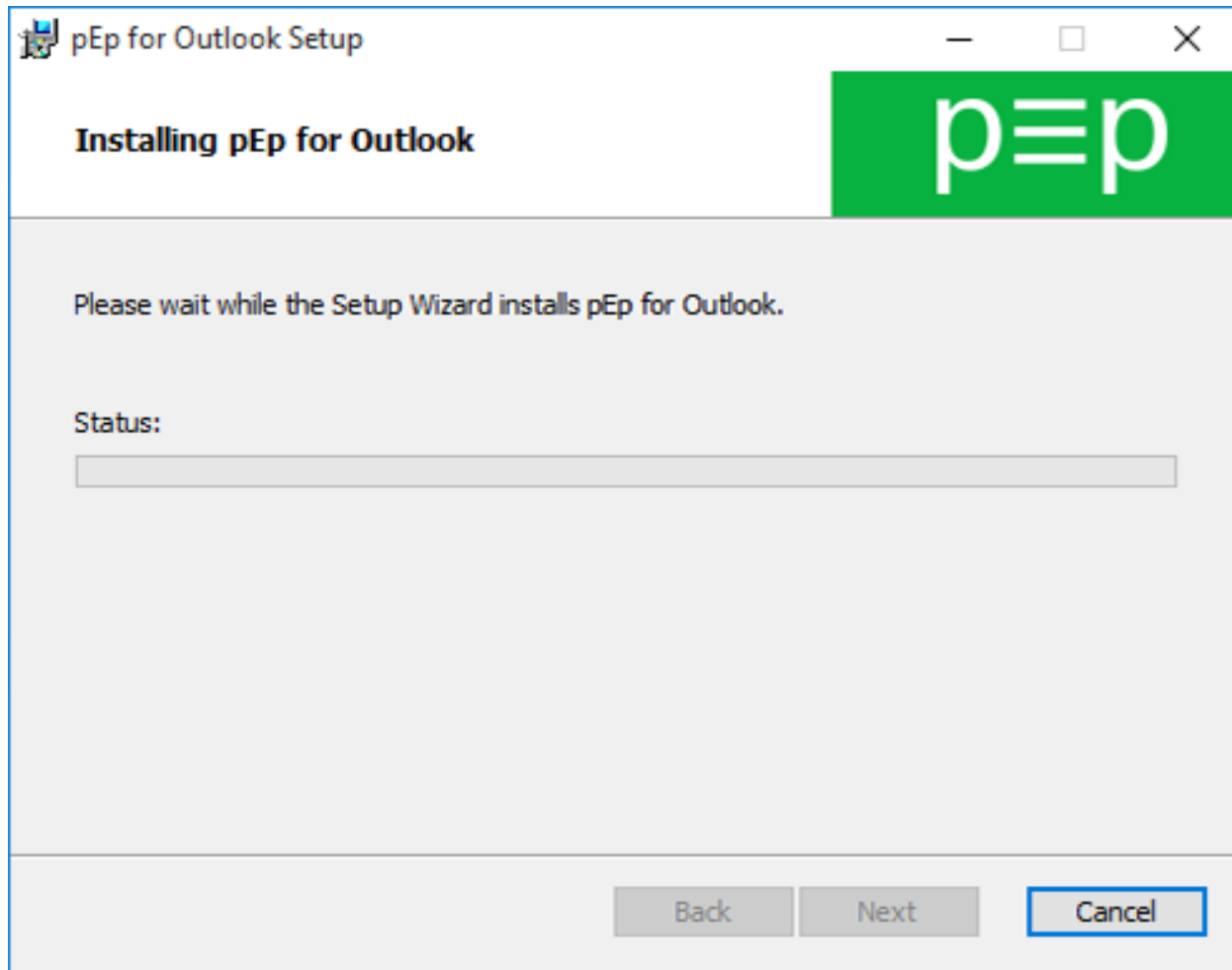
p≡p Apps: Windows/Outlook



Give
permissions

p≡p

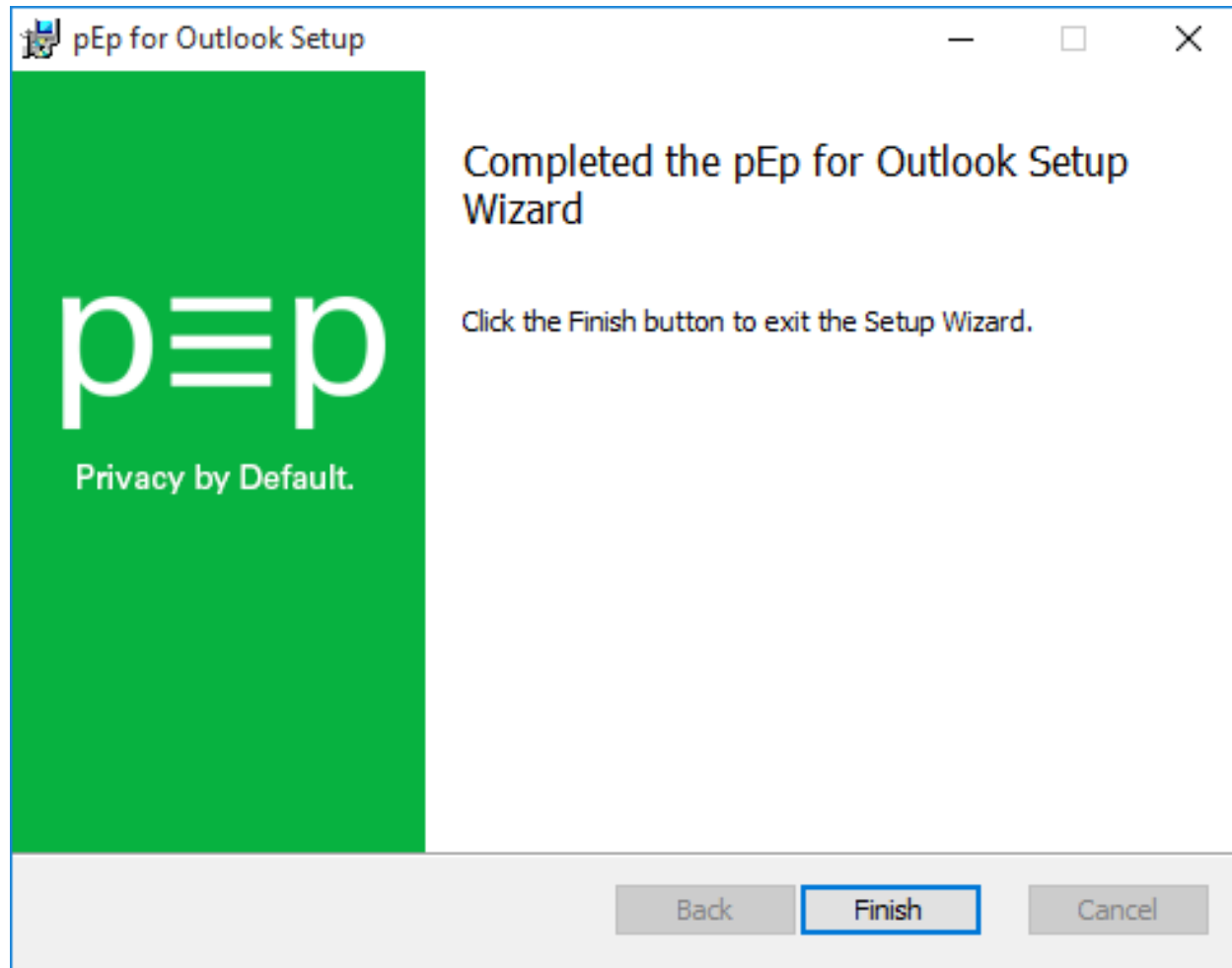
p≡p Apps: Windows/Outlook



Installing...

p≡p

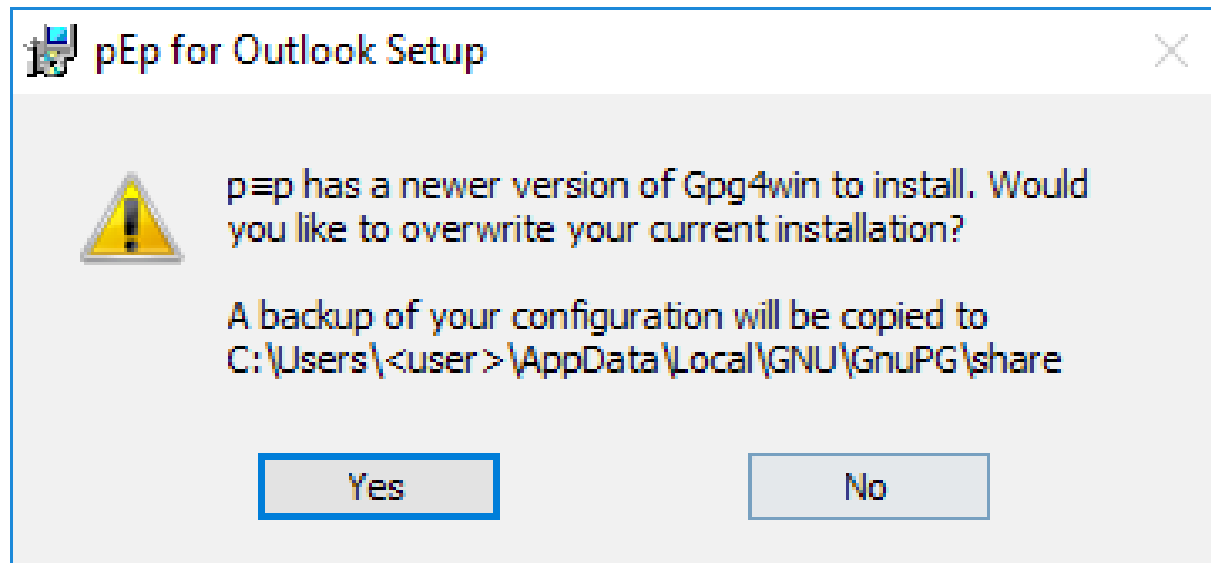
p≡p Apps: Windows/Outlook



Installation
completed



p≡p Apps: Windows/Outlook



Older version of
gpg4win is
already
installed?

Gpg4win isn't installed?

p≡p will install Gpg4win to:

C:\Program Files (x86)\GNU\GnuPG

p≡p

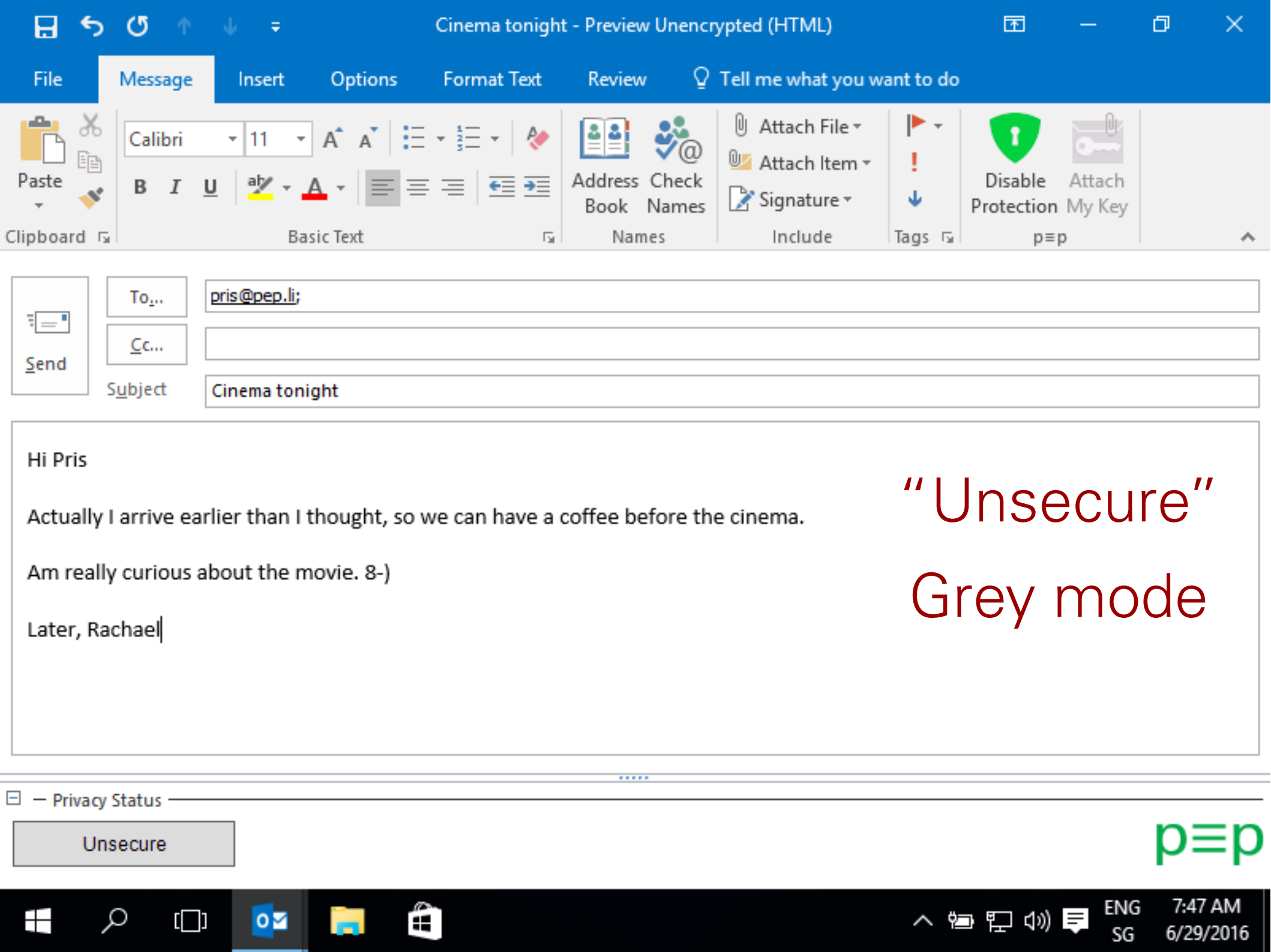
p≡p Apps: Windows/Outlook

Run in console with admin rights:

Silent /
unattended
Installation

```
msiexec /qn /i C:\pEp_for_Outlook.msi /l  
C:\pEp_install.log
```






Clipboard

Calibri 11 A A                  

Basic Text


Address Book Check Names


Attach File Attach Item Signature


Tags Disable Protection Attach My Key


Send

To... pris@pep.li;

Cc...

Subject Cinema tonight

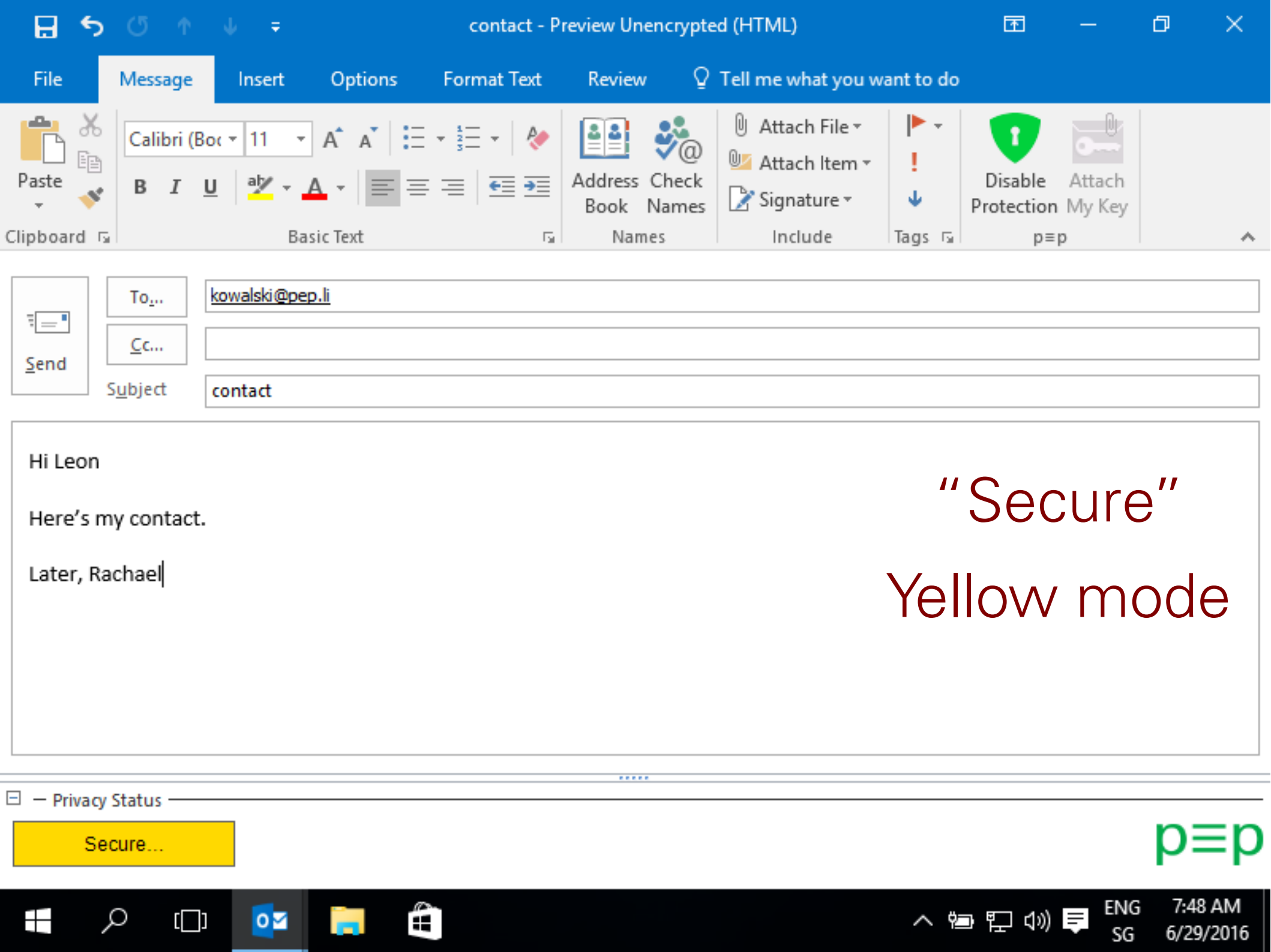
Hi Pris

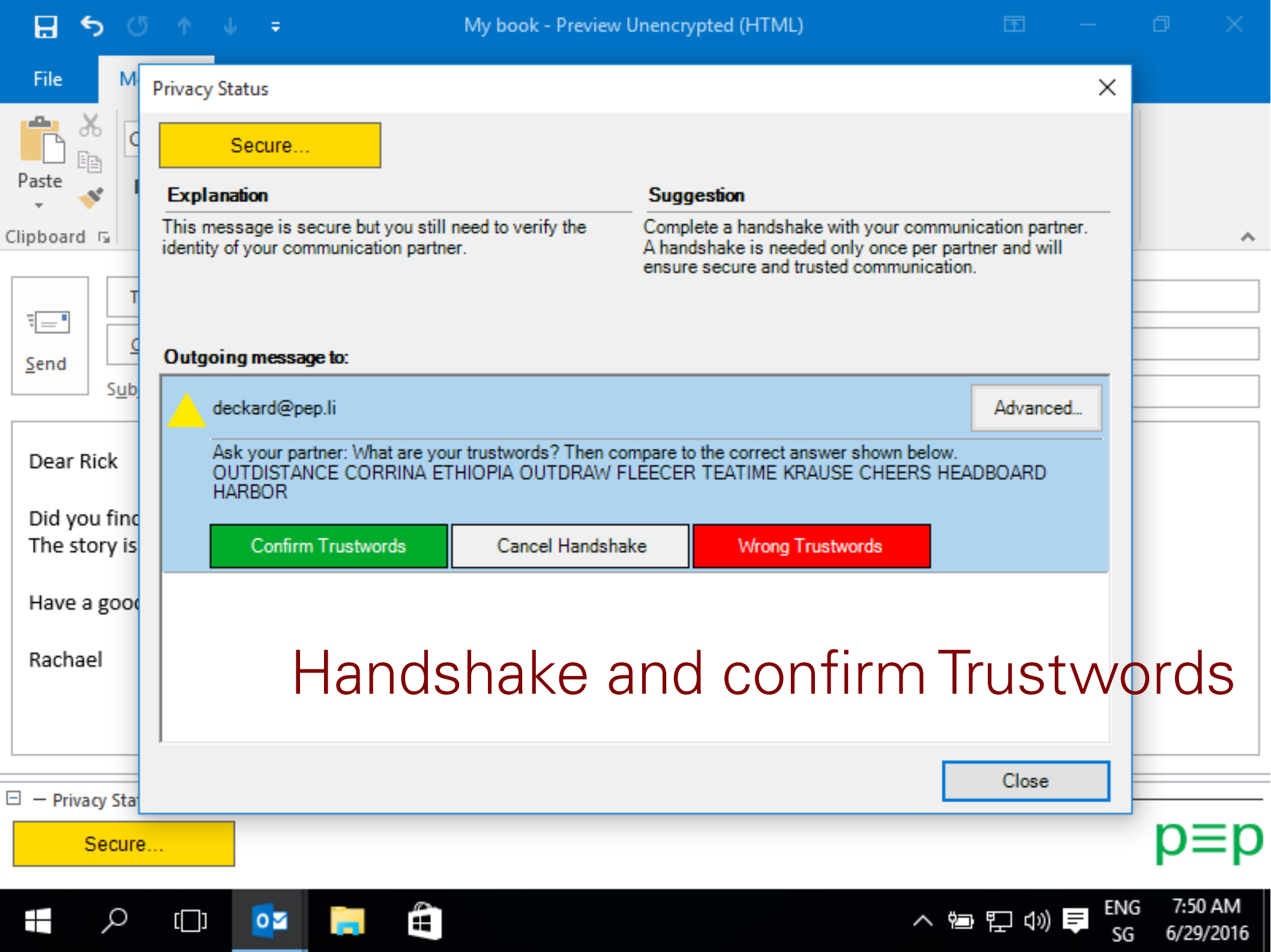
Actually I arrive earlier than I thought, so we can have a coffee before the cinema.

Am really curious about the movie. 8-)

Later, Rachael

“Unsecure”
Grey mode





Privacy Status

Secure...

Explanation

This message is secure but you still need to verify the identity of your communication partner.

Suggestion

Complete a handshake with your communication partner. A handshake is needed only once per partner and will ensure secure and trusted communication.

Outgoing message to:



deckard@pep.li

Advanced...

Ask your partner: What are your trustwords? Then compare to the correct answer shown below.
OUTDISTANCE CORRINA ETHIOPIA OUTDRAW FLEECER TEATIME KRAUSE CHEERS HEADBOARD
HARBOR

Confirm Trustwords

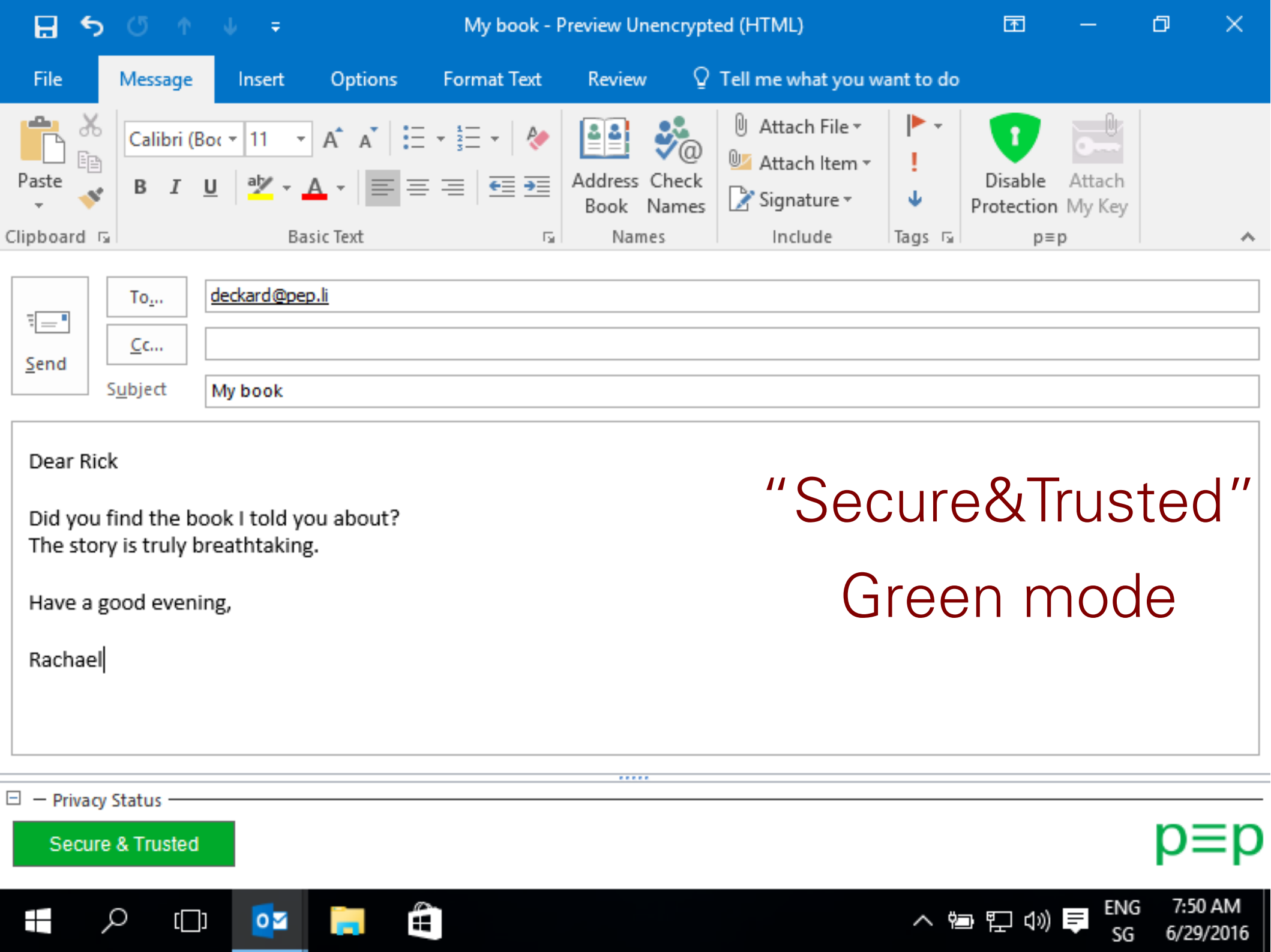
Cancel Handshake

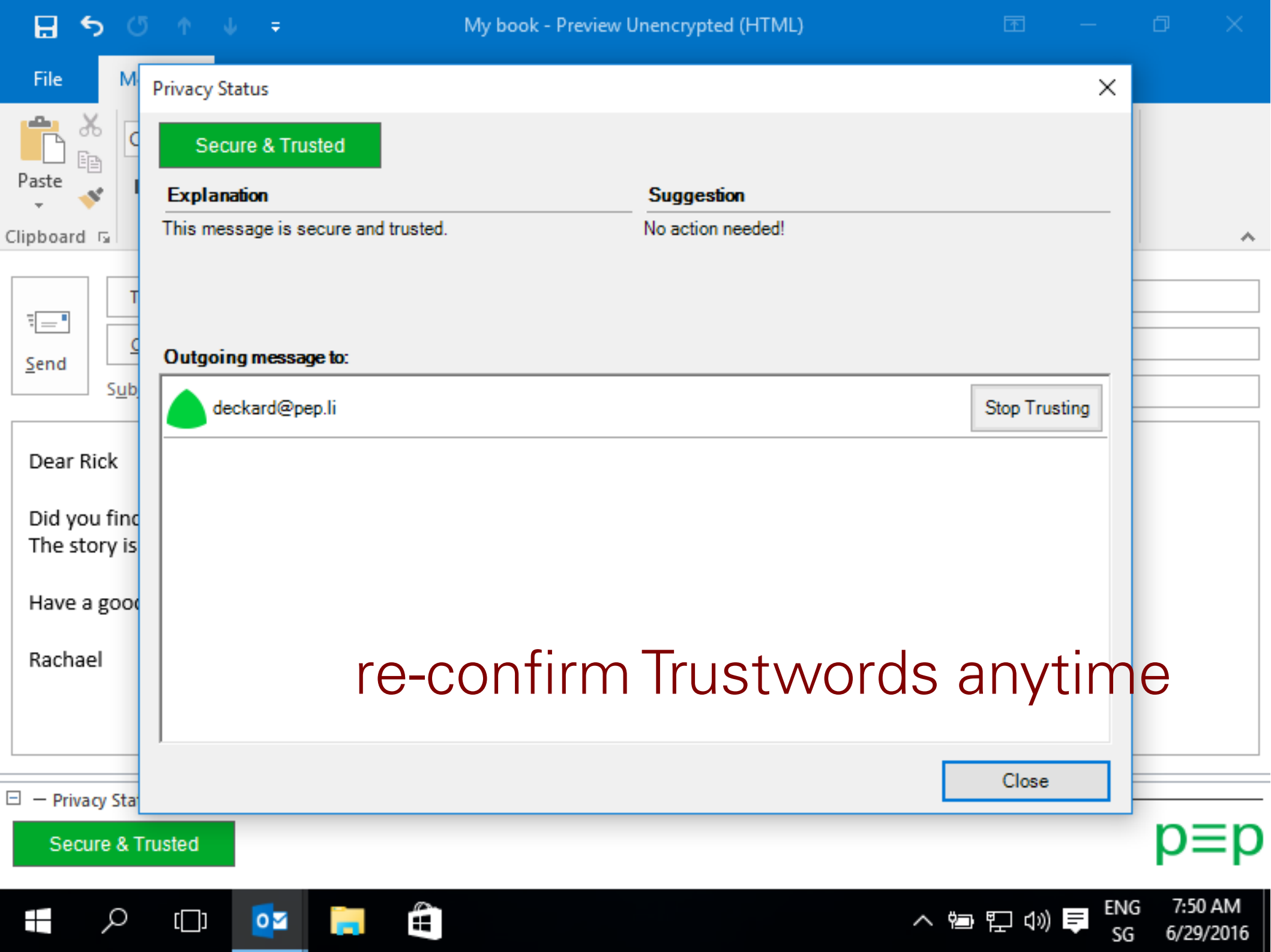
Wrong Trustwords

Close

Handshake and confirm Trustwords

pep





Privacy Status

Secure & Trusted

Explanation

This message is secure and trusted.

Suggestion

No action needed!

Outgoing message to:



deckard@pep.li

Stop Trusting

Close

re-confirm Trustwords anytime

Secure & Trusted

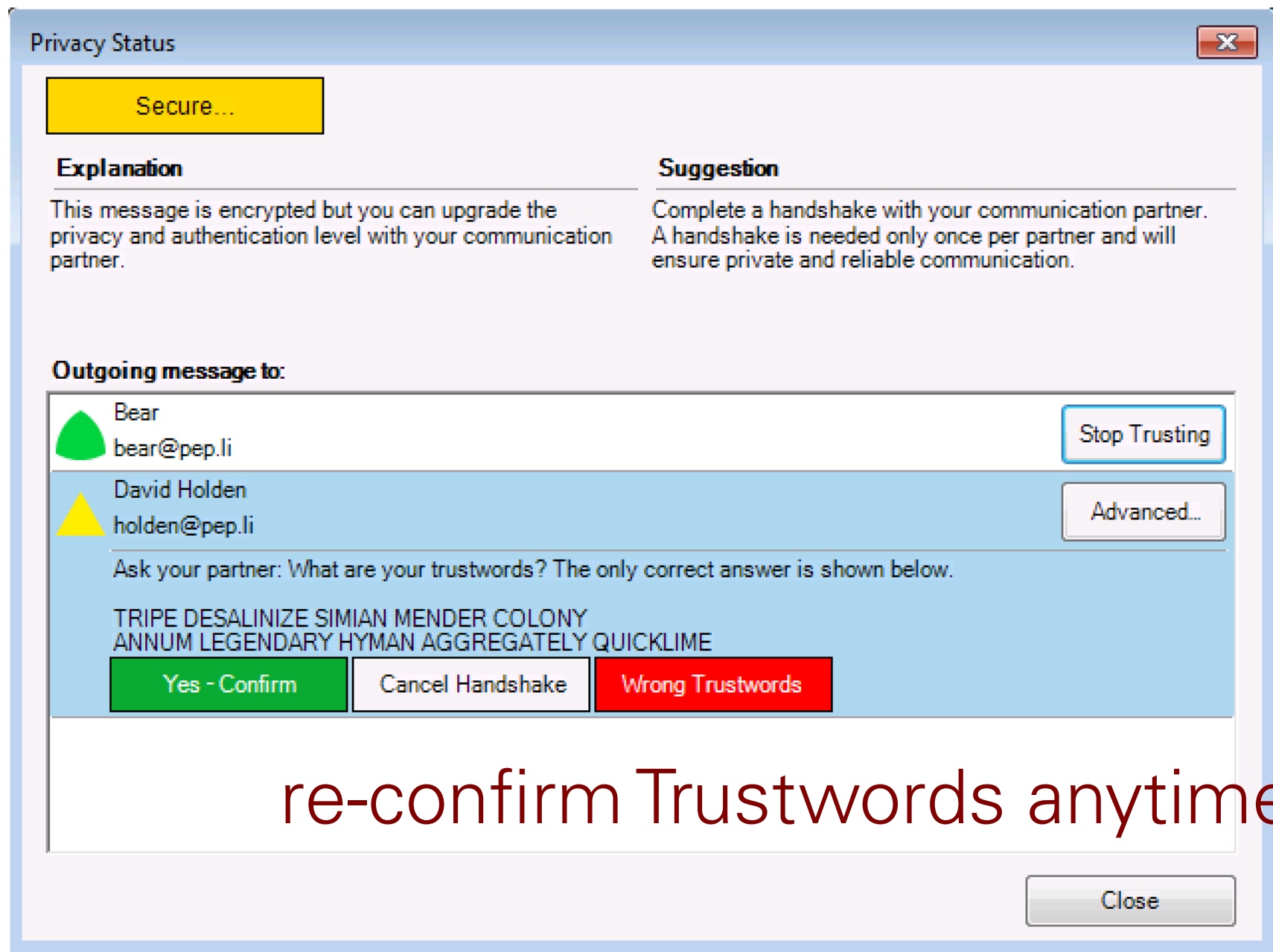
pep

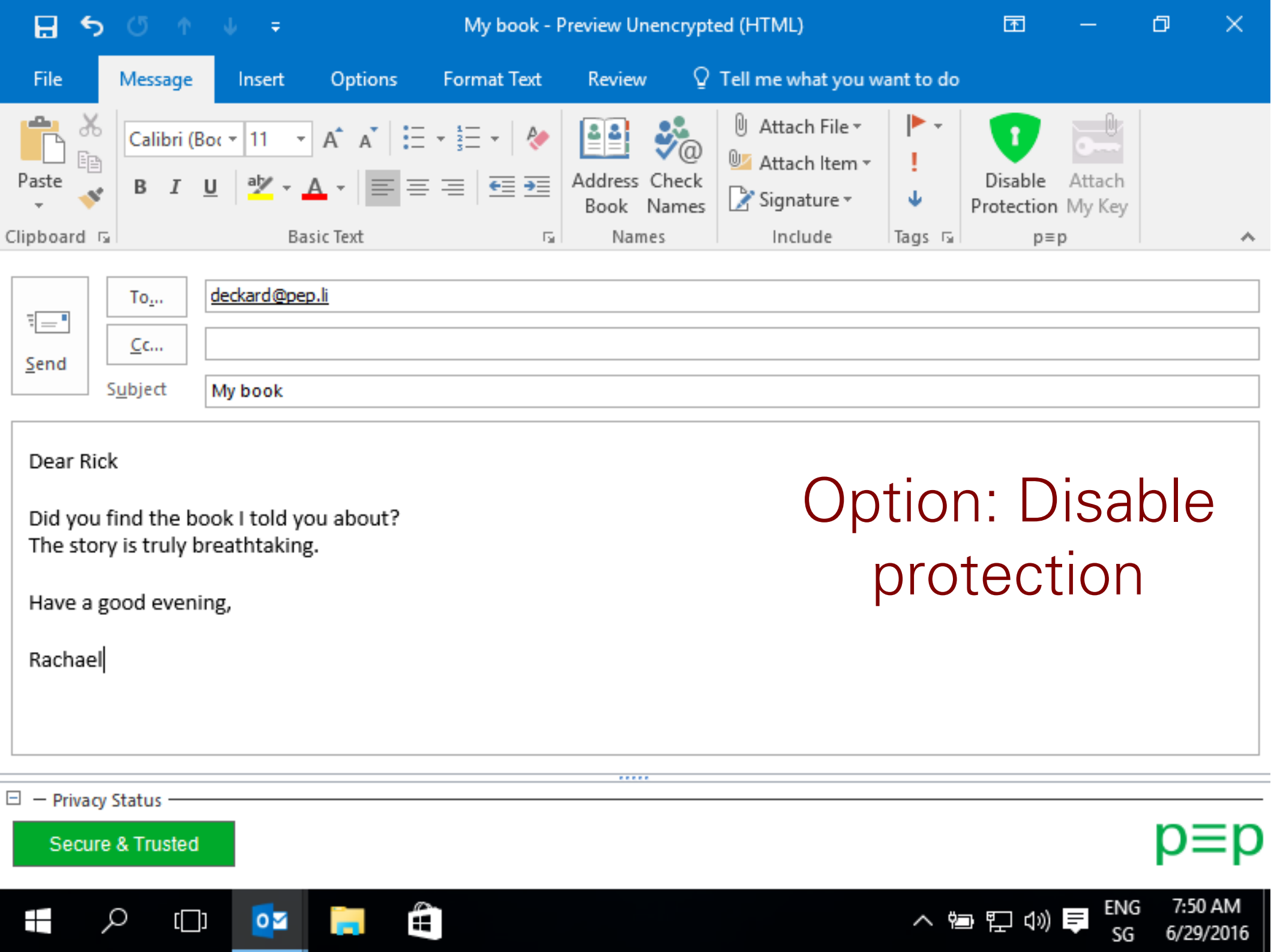


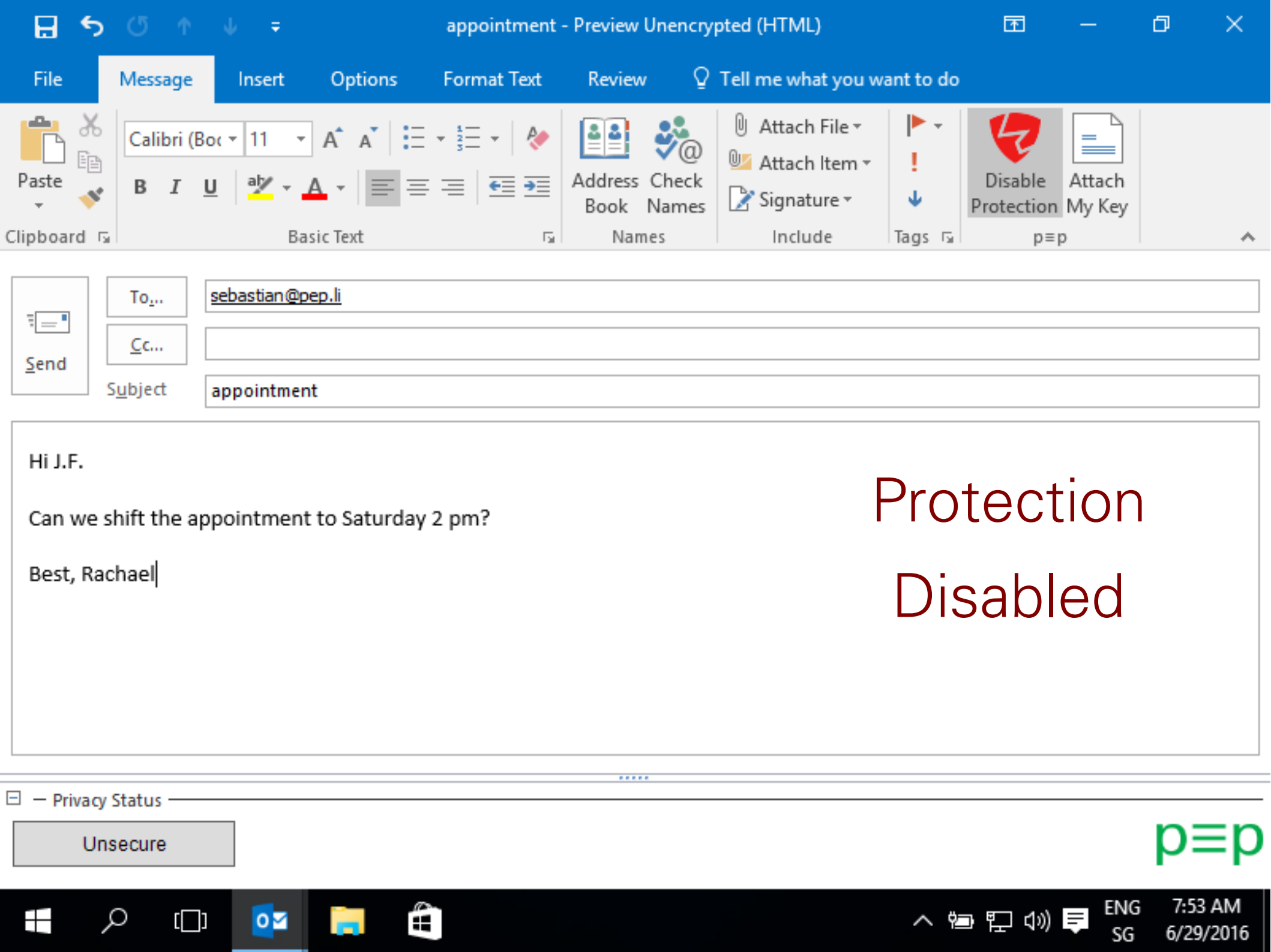
ENG
SG

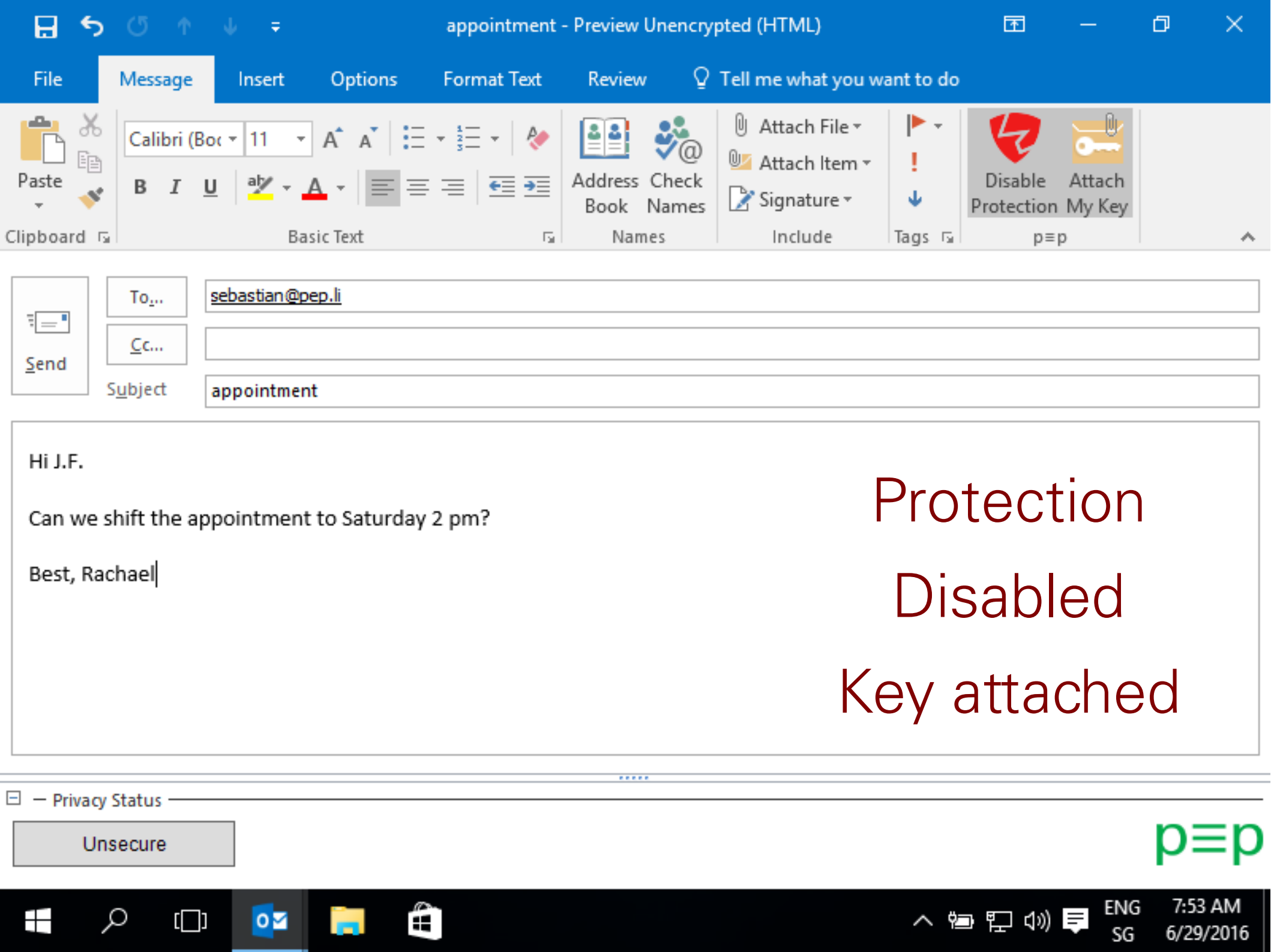
7:50 AM

6/29/2016









Paste

Clipboard

Calibri (Bo

11

A

A

B

I

U

ab

A

Basic Text

Address
BookCheck
Names

Names



Attach File



Attach Item



Signature

Include



Tags

Disable
ProtectionAttach
My Key

p≡p



Send

To...

sebastian@pep.li

Cc...

Subject

appointment

Hi J.F.

Can we shift the appointment to Saturday 2 pm?

Best, Rachael|

Protection
Disabled
Key attached

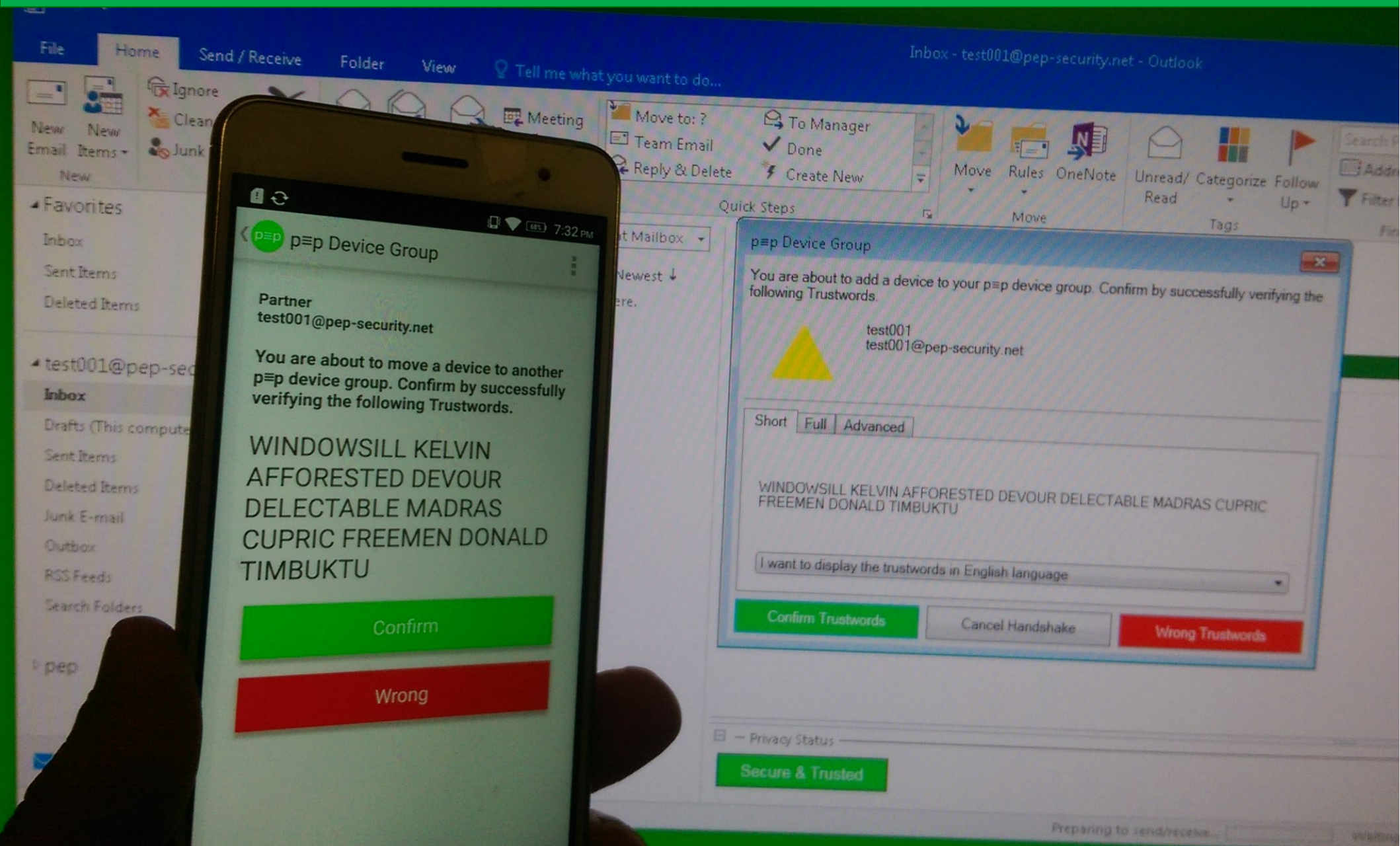
Privacy Status

Unsecure

p≡p

ENG
SG7:53 AM
6/29/2016

Android & Outlook: p≡pSync



Questions?

pretty Easy privacy:

#prettyeasyprivacy on Freenode

twitter@pEpfoundation

<https://pEp.foundation/>

<https://pEp-project.org/>

Speaker:

sva@pEp.foundation

sva@IRC (various networks)

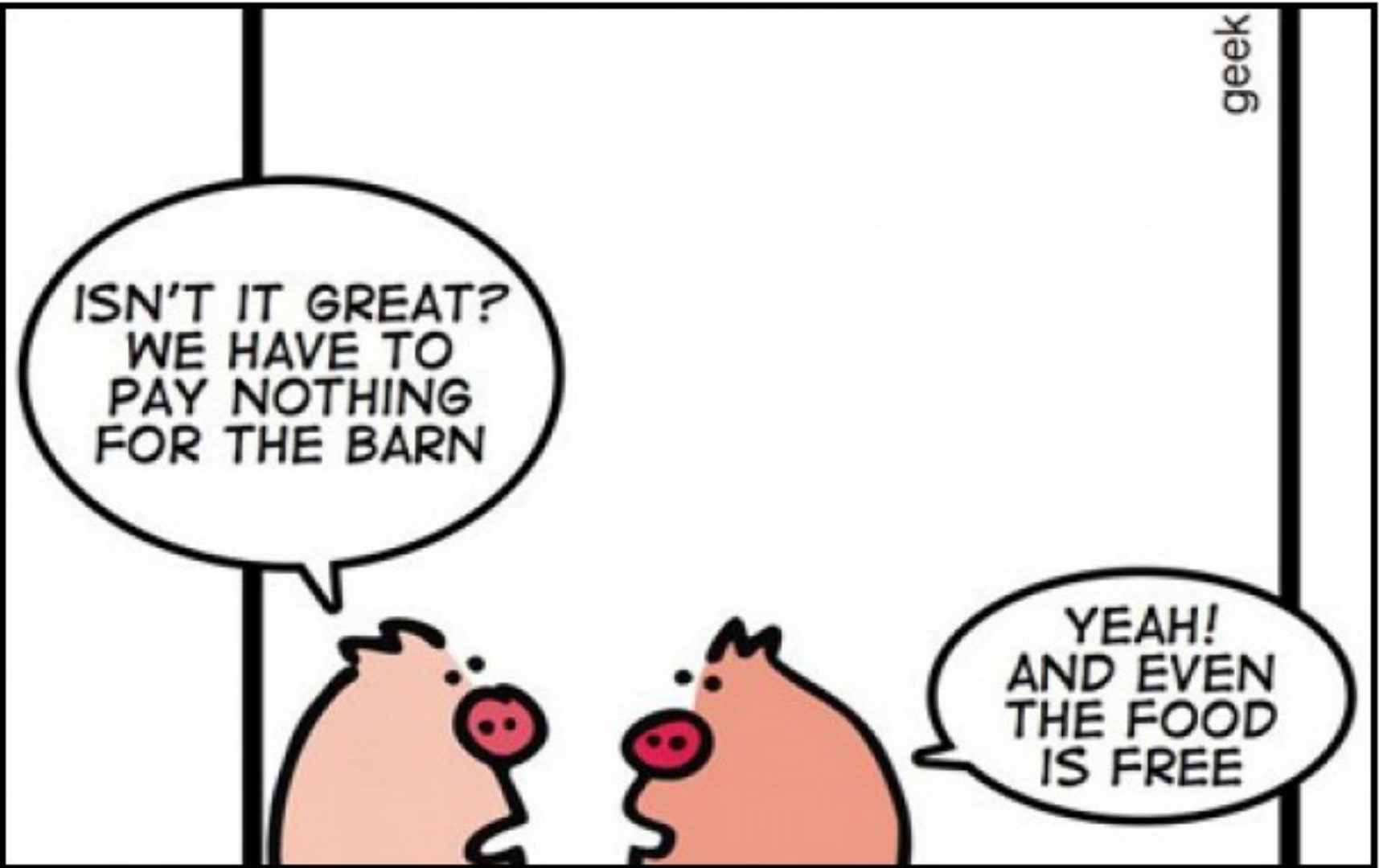
twitter@sva

Other sessions during RMLL:

Wed (taler), Thu (radar)

p≡p

p≡p



ISN'T IT GREAT?
WE HAVE TO
PAY NOTHING
FOR THE BARN

YEAH!
AND EVEN
THE FOOD
IS FREE

FACEBOOK AND YOU

If you're not paying for it, you're not the customer. You're the product being sold.