ISOC-CH Annual General Assembly: Privacy considerations and encryption

Implementing privacy by pretty Easy privacy's (p≡p) protocols and tools for mass encryption

Hernâni Marques (@vecirex),
p≡p foundation (@pEpFoundation)

hernani.marques@pep.foundation
3173 3E0C 598D 3A1C F709 55D6 CB57 3865 2768 F7E9

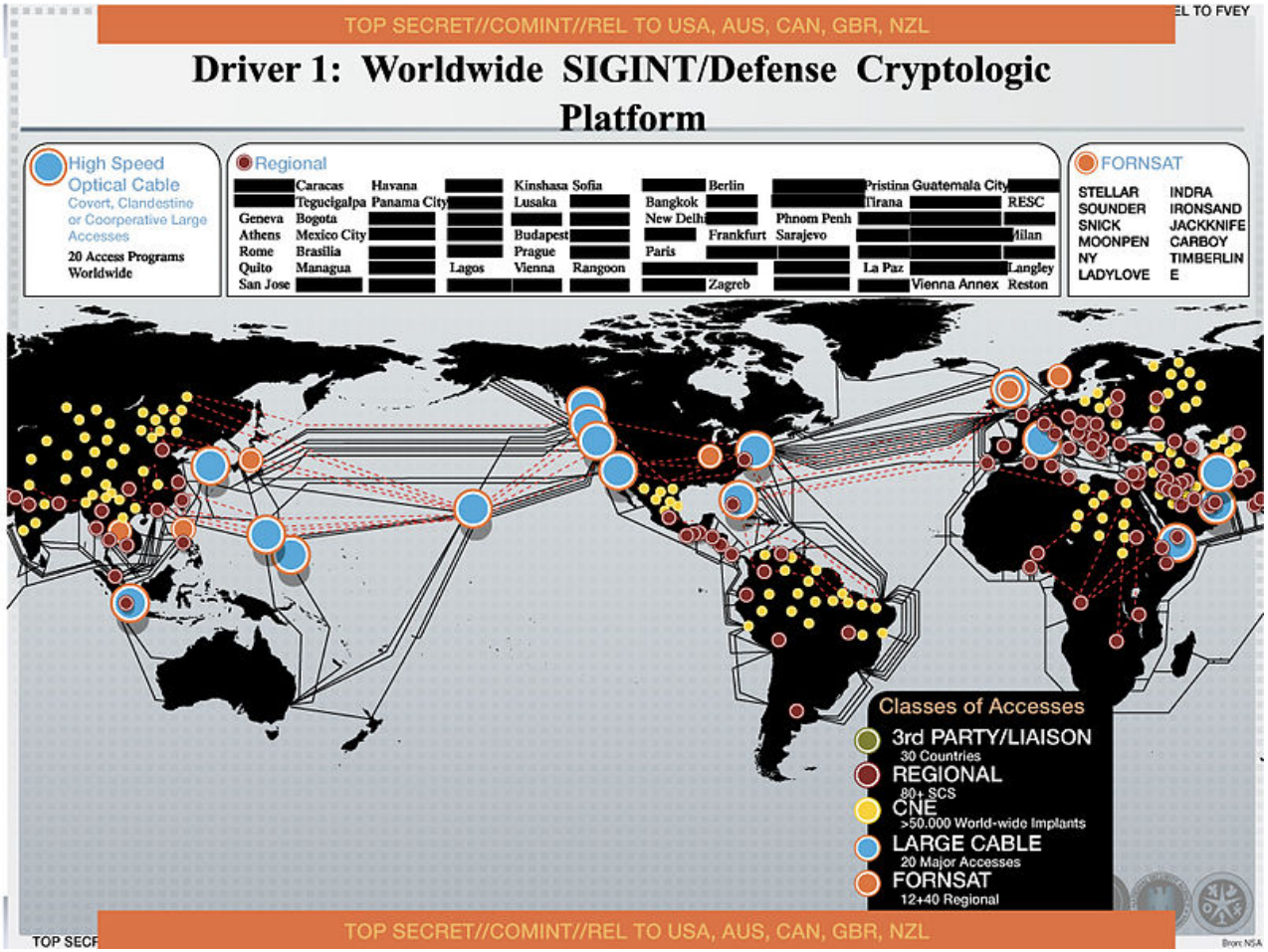
University of Bern, March 29th 2017

Overview for the next 15mins

1. Motivation to act
2. Privacy situation in CH
3. What p≡p is
4. p≡p & OpenPGP: examples
5. To be done
6. Commmunity work
7. Your turn

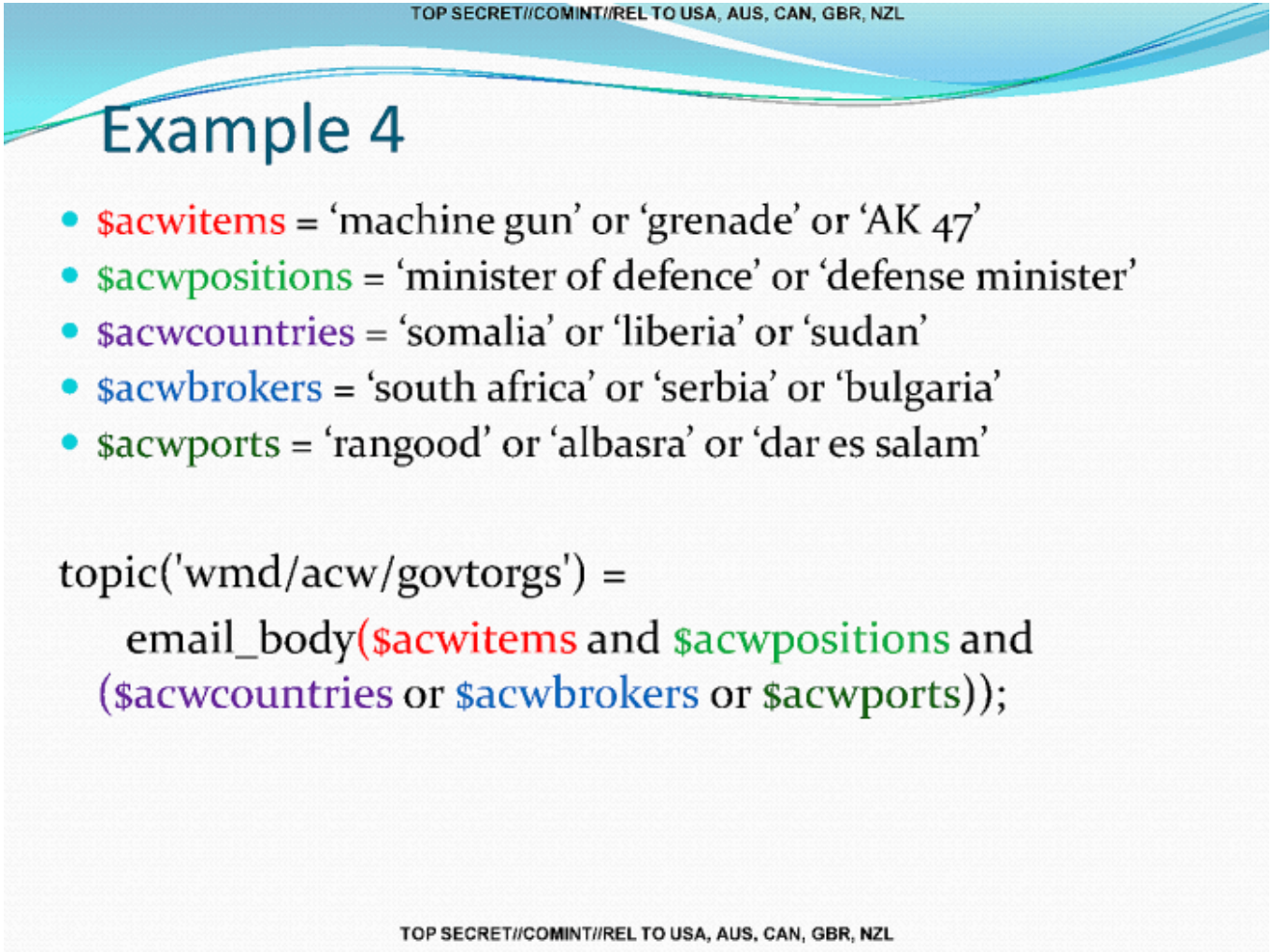
The mindset we face

In a general global context

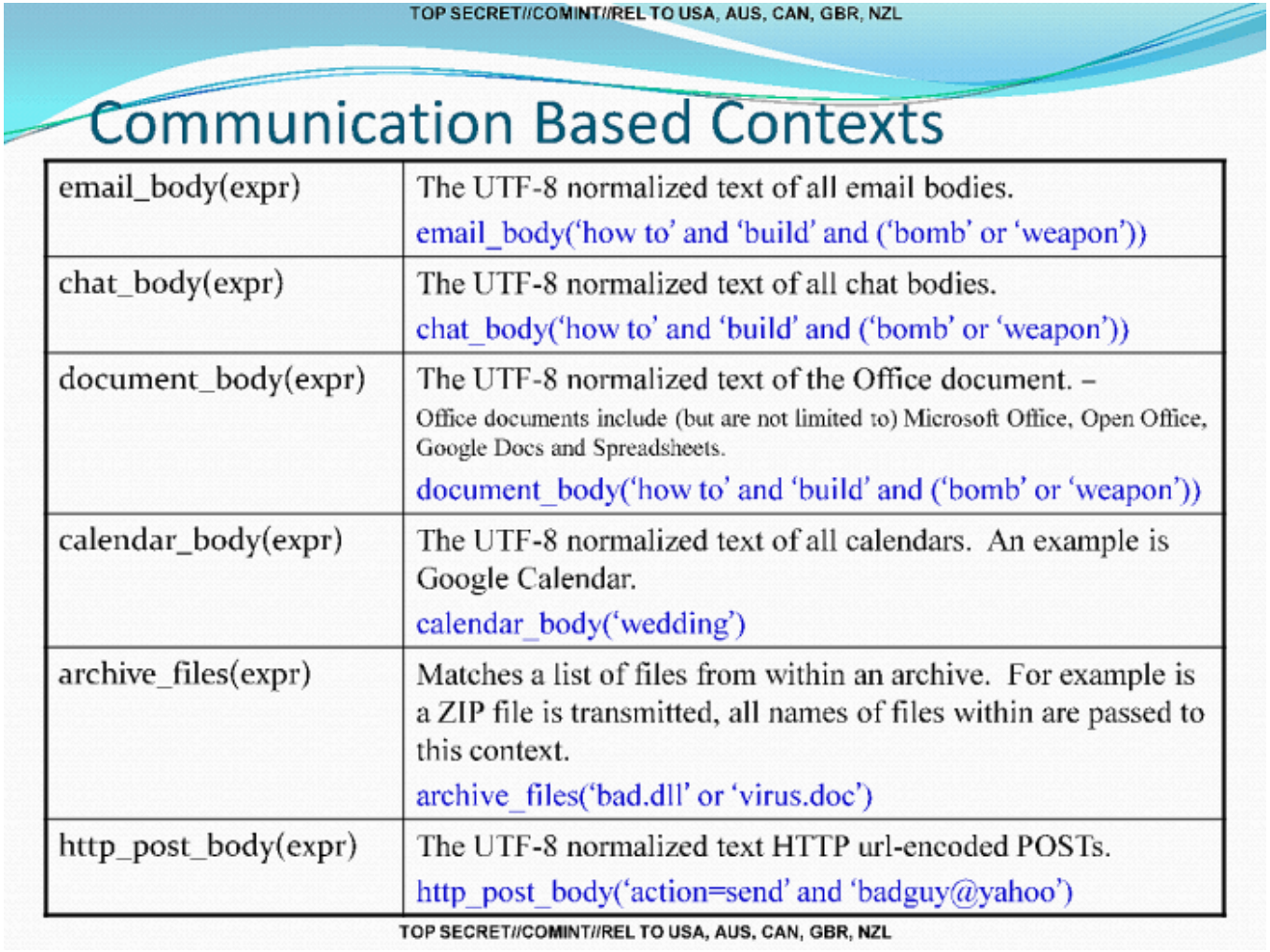


In a general (Swiss) local context

In an email context



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. email_body('how to' and 'build' and ('bomb' or 'weapon'))
chat_body(expr)	The UTF-8 normalized text of all chat bodies. chat_body('how to' and 'build' and ('bomb' or 'weapon'))
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. document_body('how to' and 'build' and ('bomb' or 'weapon'))
calendar_body(expr)	The UTF-8 normalized text of all calendars. An example is Google Calendar. calendar_body('wedding')
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. archive_files('bad.dll' or 'virus.doc')
http_post_body(expr)	The UTF-8 normalized text HTTP url-encoded POSTs. http_post_body('action=send' and 'badguy@yahoo')

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

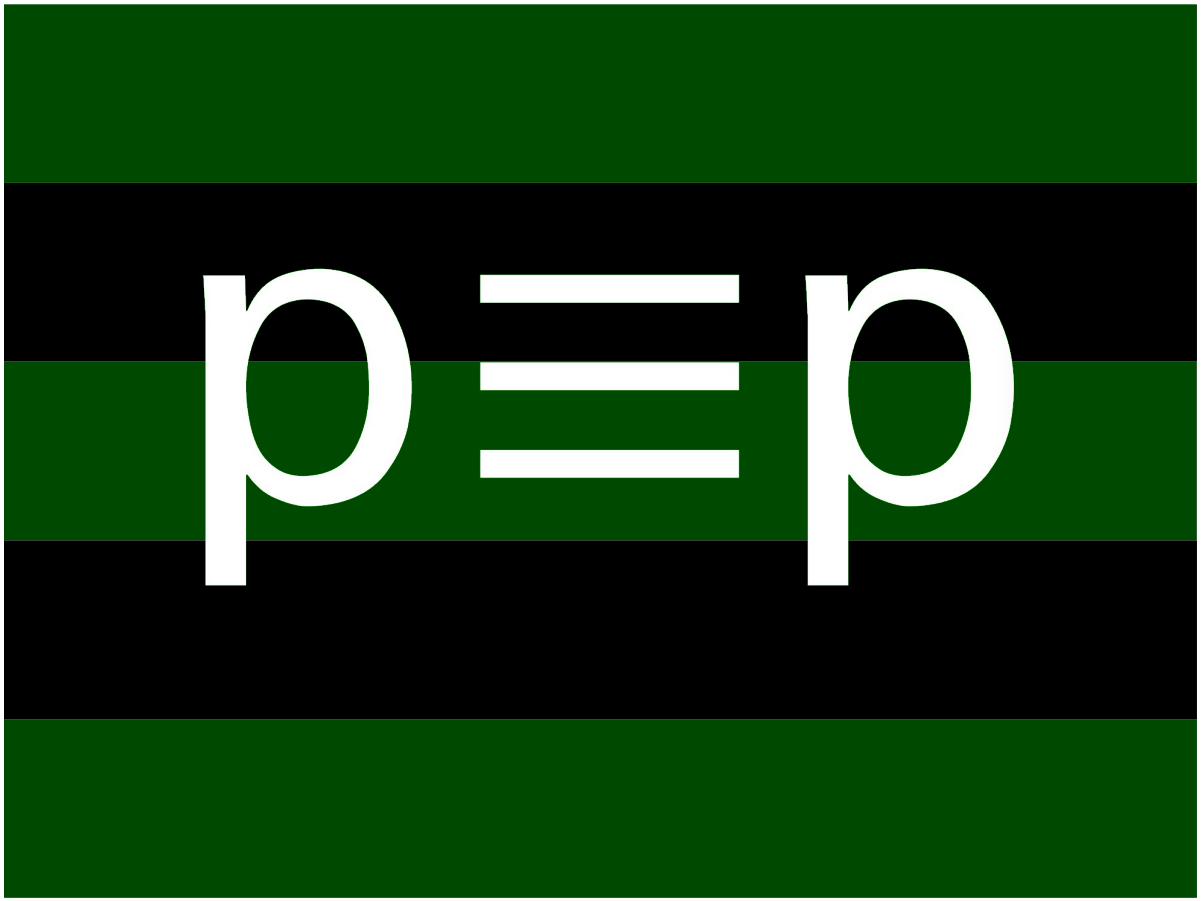
Data retention for LI purposes: BÜPF / LSCPT

- **Today:** Data retention of 6 months for **access providers** (including mobile phones).
- **2018**: Data retention of 6 months *additionally* for **service providers**; private providers of Internet access (firms, schools, associations etc.) must give at least access to their infrastructure, such that the state can install implants . . .
- **Sep 2017:** Also the Swiss secret service (NDB) can access all data accessible by the BÜPF law, i.e. (mis)using law-enforcement. (Today the NDB can “just” query through BÜPF / LSCPT law whom a hard selector belongs to (e.g., a phone number or IP address)).

More Mass Surveillance & Data retention for the NDB: ZNDG / VEKF / NDG

- **Before 2013**: *Onyx* was built as of 1999 illegally and passed in parliament under the military budget as “multi-purpose building” for CHF 45 millions. *Onyx* works in full operation since 2005 – for 7 years (!) illegally.
- **Today**: As of 2012 legal basis (ZNDG / VEKF) was created for *Onyx* to operate: data from mass surveillance on SAT-based communications can be retained for 1.5 (content) and 5 (!) years (metadata).
- **Sep 2017:** The secret service law NDG *additionally* introduces cable-based mass surveillance. In the corresponding executive order NDV, once again, the same data retention rules are imposed: 1.5 and 5 years for content and metadata, respectively.

p≡p = pretty Easy privacy



p≡p is . . .

- a set of rules describing how to carry out encryption automatically for the user, i.e. a protocol.
- a cross-platform abstraction (with an actual reference implementation) 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.

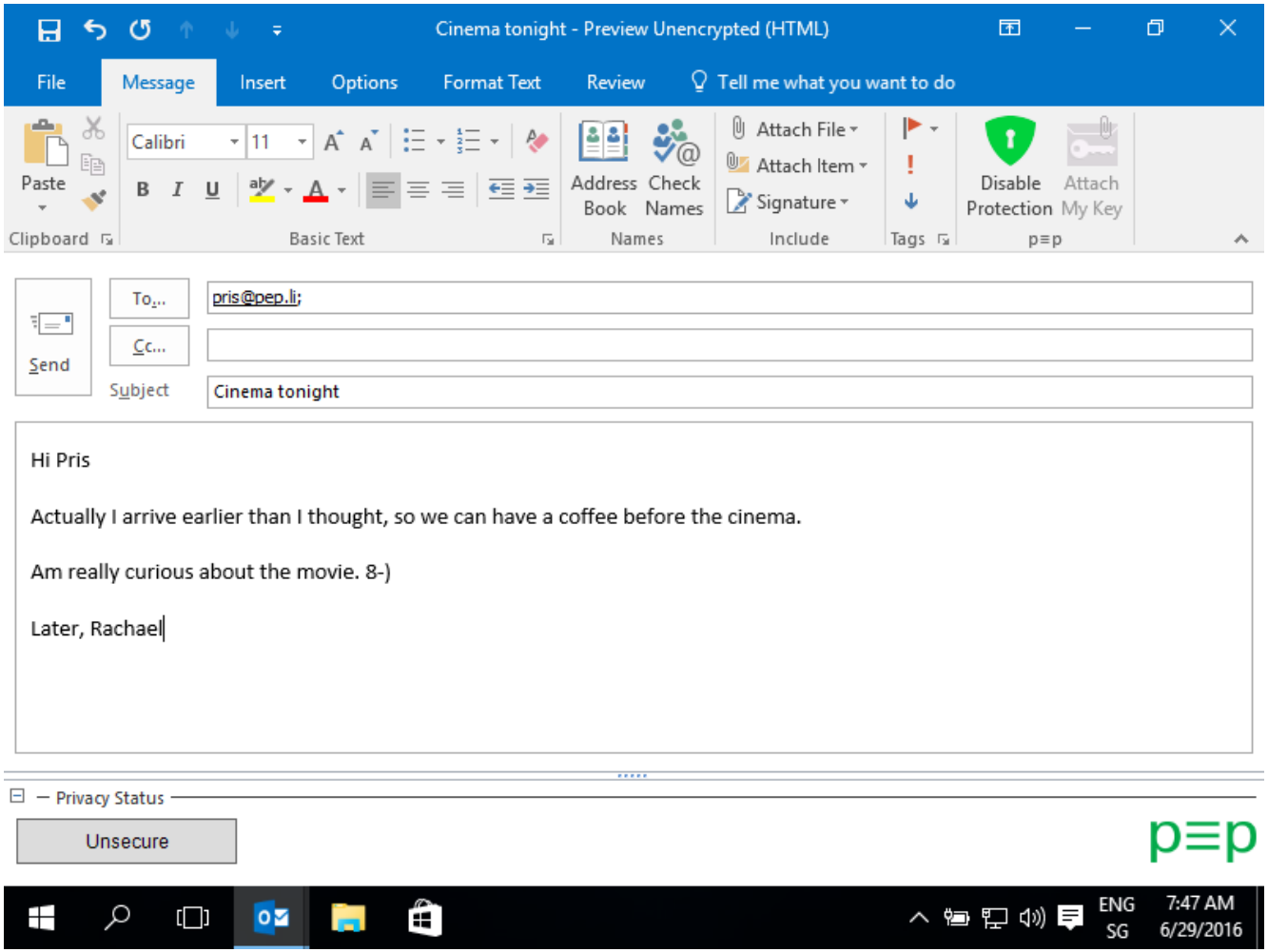
p≡p is **not** . . .

- 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.
- yet another tool just for encrypting email: that's just the beginning and not the end.
- storing any user data and profiles.
- specific to any service provider.
- imposing any restrictions on identity choices (like phone numbers, specfic email addresses or other URIs).
- trading off privacy for security – privacy has always highest priority.

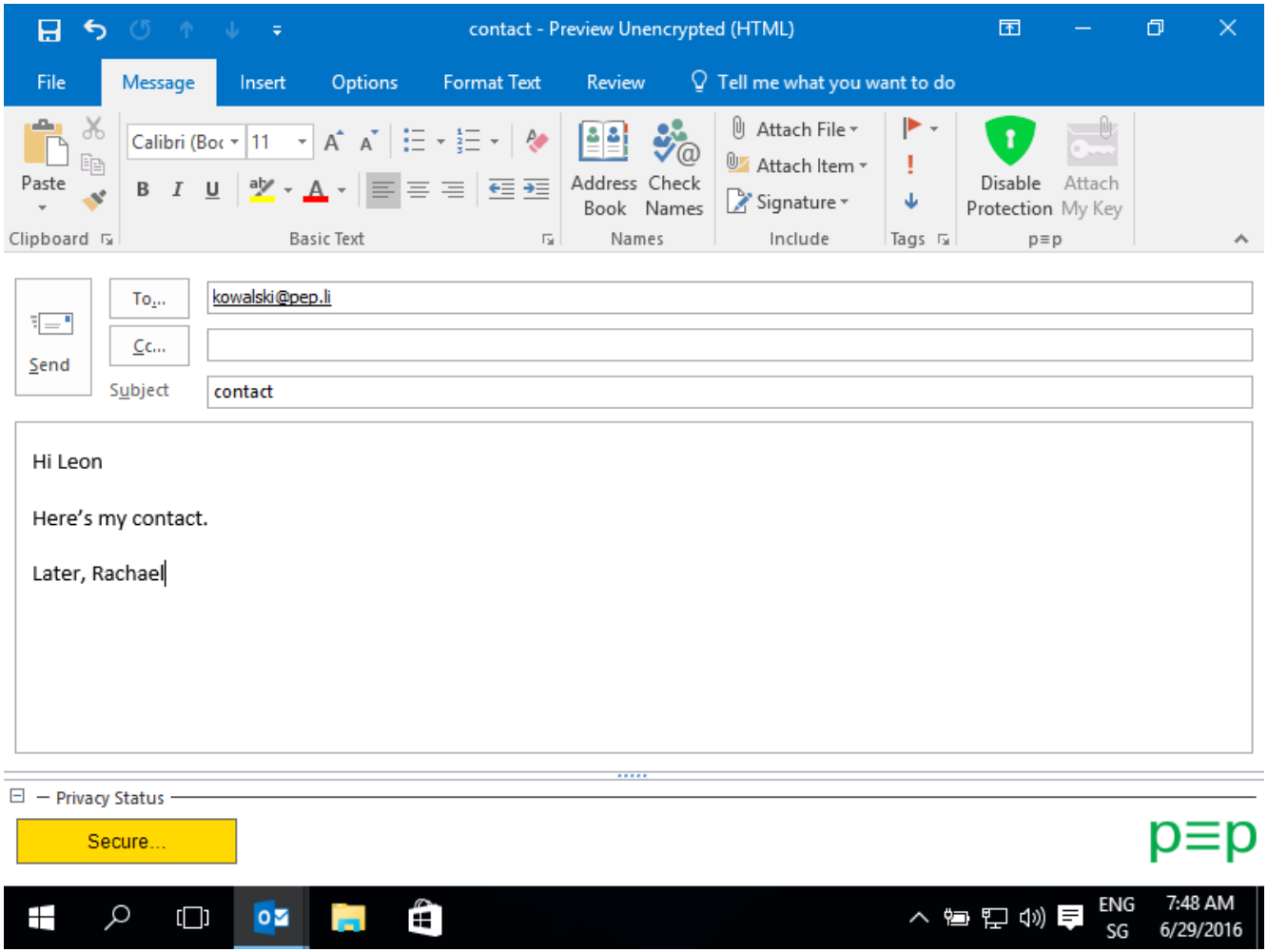
p≡p differences to current OpenPGP MUAs

- Keyservers are never used by default to prevent leakage of a peer's social graph (by signings and queries) and MITM attacks (re-encyption).
- 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.

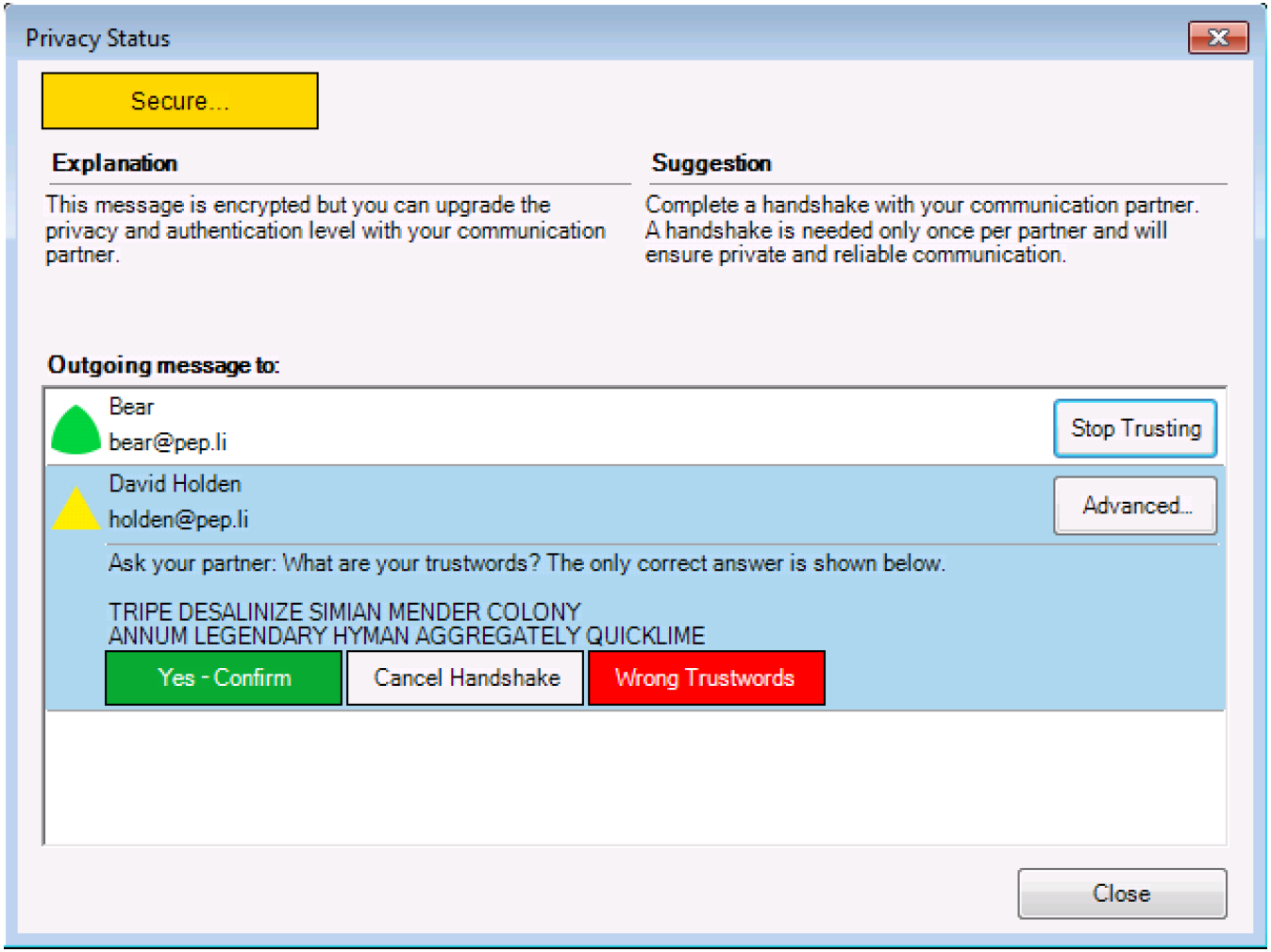
p≡p for Outlook: first email (unsecure)



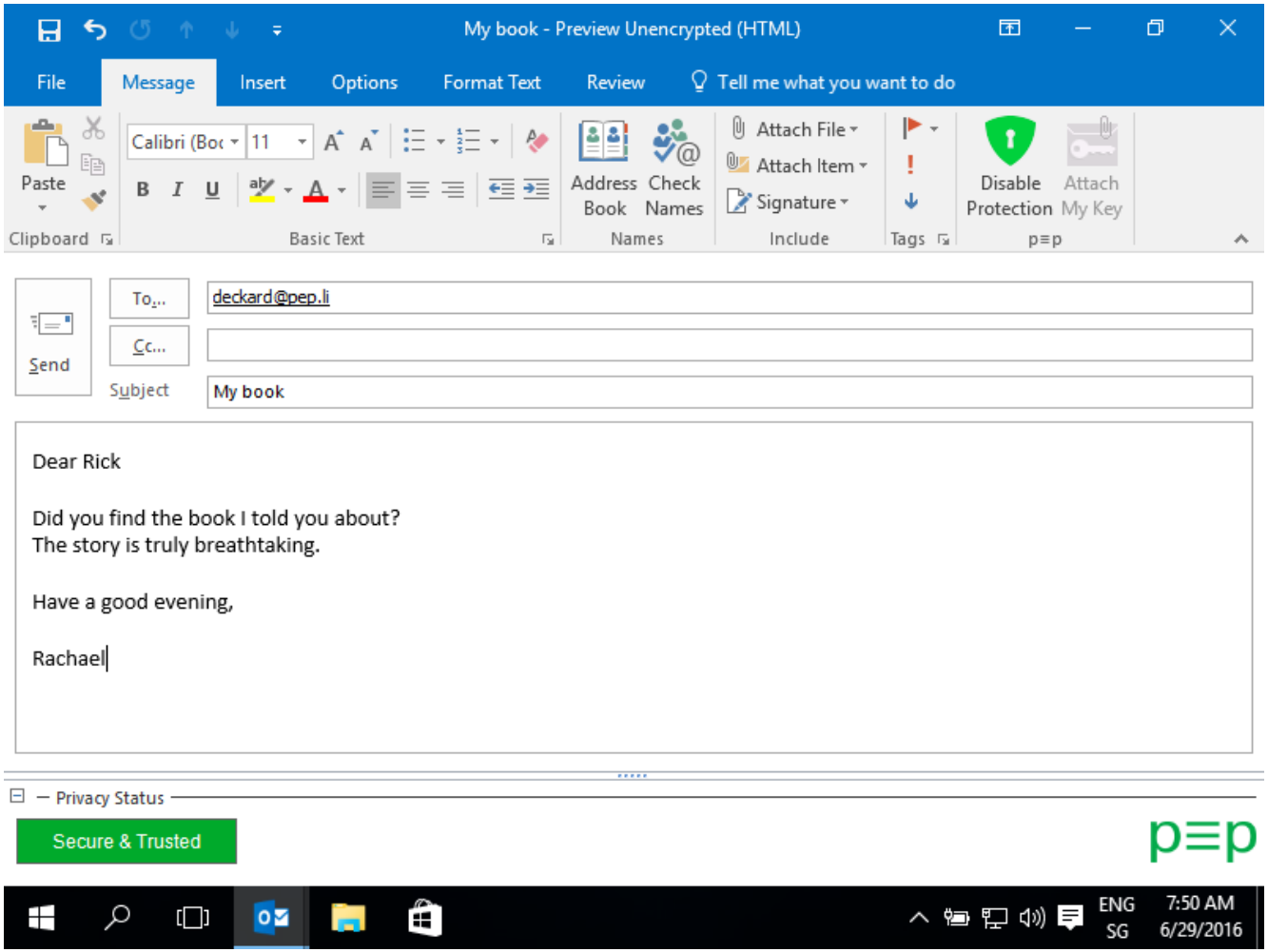
p≡p for Outlook: second email (secure)



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 **now** with ISOC Switzerland (ISOC-CH) – focussing on the open standardization of p≡p's protocols through participation in the Internet community (IETF).

Questions