

Opportunistic Encryption of Email and Messaging

ARTAREA @ IETF-102, Mon July 16, 2018

draft-birk-pep-02

draft-marques-pep-email-01

draft-marques-pep-handshake-00

draft-marques-pep-rating-00

draft-birk-pep-trustwords-02

Bernie Hoeneisen / Hernâni Marques



Privacy by Default.

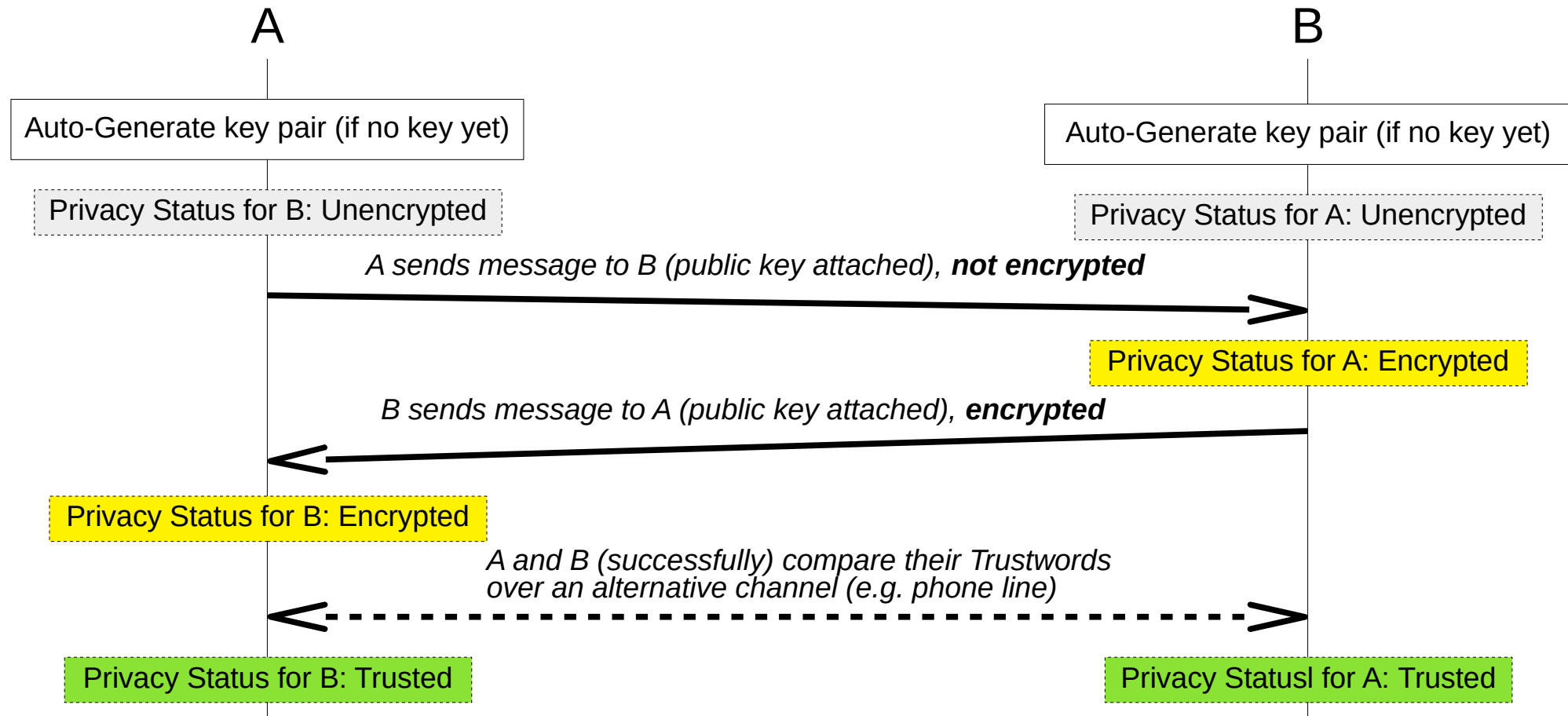
Background

- We aim to make text communications (i.e. email, chat, ...) **private by default**
- “Good” tools for privacy already exist (e.g. PGP/OpenPGP)
- **However:**
 - Most users are unable to use existing encryption tools like GnuPG (properly)
- Need to fix this usability challenge by automation
- Not just “good”, but **easy** privacy

pEp – pretty Easy privacy

- The pEp architecture consists of several building blocks
- Existing RFCs are used whenever available (and usable)
- Some pieces are currently missing (or incomplete)
- We intend to document the missing pieces in the IETF

Example Msg. flow (simplified)



draft-marques-pep-email

- Goal
 - Define missing pieces for email
- Motivation
 - Current systems do not encrypt all privacy-sensitive information (e.g. subject)
- Main use-case
 - Automatically encrypted email in opportunistic encryption scenarios
- Method
 - Strict message formats for privacy and integrity
 - Automatic key generation, distribution, and import

pEp Email Format 2

Outer message (Subject: pEp)

Inner message: encrypted original email

Original headers & content

Public key

draft-marques-pep-rating

- Goal
 - Easy understandable representation of Privacy Status
- Motivation
 - Reveal Privacy Status of a communication to users
- Main use-case
 - Presentation of Privacy Status between users
 - Presentation of Privacy Status of particular messages
- Method
 - Defining different Privacy Ratings
 - Mapping Privacy Ratings to colors (traffic light semantics)

draft-marques-pep-handshake

- Goal
 - Define easy authentication process for communication partners
- Motivation
 - For most users current authentication methods are too cumbersome and therefore rarely (correctly) applied
- Main use-case
 - Process to establish trust between communication partners
- Method:
 - Mapping of combined fingerprints to human readable output using Trustwords

draft-birk-pep-trustwords

- Goal
 - Mapping of hexadecimal stings to natural language words
 - Public registration of Trustwords in different languages
- Motivation
 - Word lists need to be the same for every implementation
- Main use-case
 - Easy comparison of fingerprints or handshake results to establish a trust relationship
- Method
 - Create IANA registry

Running Code: www.pep.software

- p≡p for Outlook (release: add-on)
- p≡p for Android (release: app)
- p≡p for Thunderbird (release: as Enigmail 2.0 add-on with p≡p integration)
- p≡p for iOS (internal beta)

Where can IETF help?

- Improve compatibility to what's out in the wild
- MIME-based message formats
- Define missing URI schemes
- IANA registry to support trust establishment
- Private Key Synchronization
 - to fit multi-device scenarios;
in email via ActiveSync/IMAP
- ...

Places to touch base / join in

- Mailinglist discussion:
 - dispatch@ietf.org
- Other communication channels:
 - IRC: [#PrettyEasyPrivacy](irc://irc.freenode.net)
 - Web forum: <https://pep.community/>
- Contact us directly:
 - hernani@pep.foundation / bernie@ucom.ch

Questions / Discussion