Opportunistic Encryption of Email and Messaging

dispatch @ IETF-101, Mar 20 2018

draft-birk-pep-01

Bernie Hoeneisen / Hernâni Marques

p≡p

Privacy by Default.

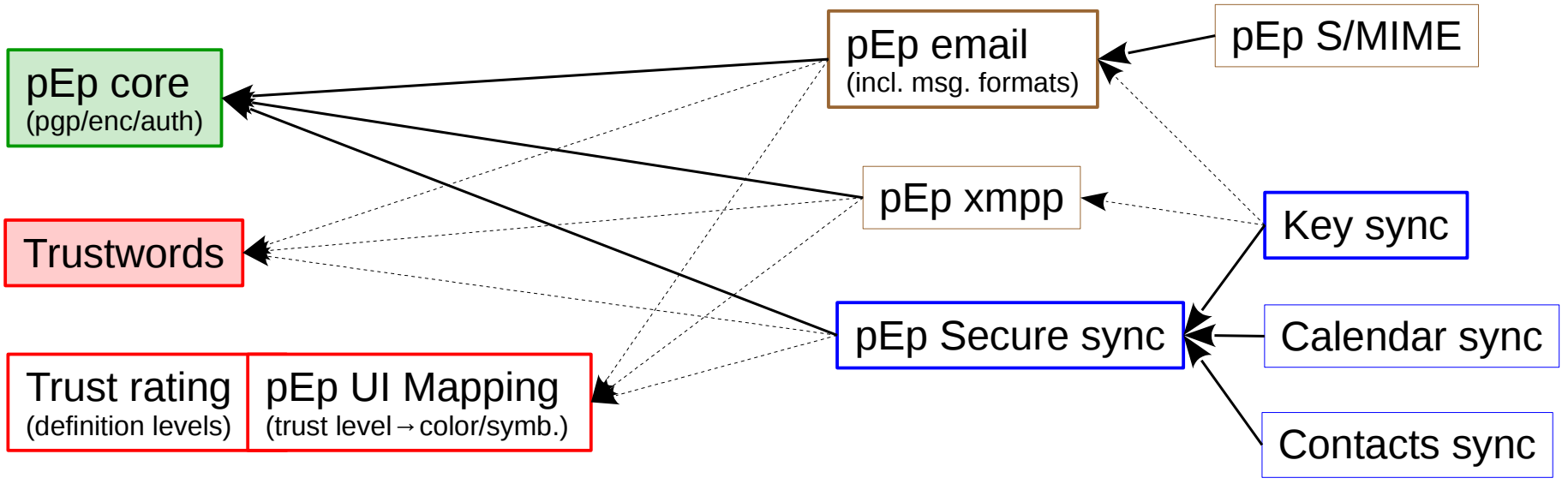
Privacy by Default

- We aim to make all communication (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 and Standards are used whenever available (and usable)
- Some pieces are currently missing (or incomplete)
- We intend to document the missing pieces as RFCs

pEp I-Ds Dependency Graph



Legend:

core

Establishing trust relationship / visualizing trust levels

Secure and decentralized synchronization

pEp Applications

depends on

uses

I-D exists

I-D coming soon

Where can IETF help?

- MIME based message formats (message in message encapsulation)
- Public/Private Key Synchronization (between different User's devices)
- Base protocol mapping for email, Jabber, ...
- URI schemes for missing message addressing
- IANA registry to support trust establishment
- and more...

Demonstration of pEp

- Wanna know more about how this works?

- Short demonstration of the running code:
  - **Wed 21.03.2018 / 10:30-11:30**
  - Meeting room **Waterloo**

Questions / Discussion