Background

- 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

- pEp core (pgp/enc/auth)
- pEp email (incl. msg. formats)
- pEp S/MIME
- pEp xmpp
- pEp sync
- Contacts sync
- Calendar sync
- Trust sync
- Trustwords (IANA Registry)
- Trust rating (definition levels)
- pEp UI Mapping (trust level → color/symb.)
- pEp Handshake
- Trust sync

Legend:
- Secure and decentralized synchronization
- pEp Applications
- depends on
- uses
- I-D exists
- I-D coming soon
Trustwords (1/3)

- Motivation
  - Word lists are easier to understand for users than hexadecimal codes

- Main Use Case
  - Easy comparison of fingerprints or handshake results to establish a trust relationship

- Target audience:
  - Ordinary human users

- Method:
  - Mapping binary to human readable output using word lists
Trustwords (2/3)

- Example:
  - Instead: F482 E952 2F48 618B 01BC 31DC 5428 D7FA ACDC 3F13 → dog house brother town fat bath school banana kite task

- Previous related work includes:
  - RFC 2289
  - RFC 1751
  - RFC 1760
  - PGP Word List
Trustwords (3/3)

- New work is different:
  - Map **16-bit** of data to Trustwords (as opposed to 8-bit only)
  - **Trustwords** are **only read** on an side channel (e.g. phone) **by humans**
  - Concept open to any **language** (as opposed to English only)

- Establish IANA Registry for Trustwords lists in different languages
  - Similar concept as RFC 6117
Issues

- So far the following issues popped up (on saag mailing list):
  - Translations between Trustwords
    - Use Case?
  - Ensure it contains innocuous words only (no swear words)
    - Combinations
Proposal to go forward

- Continue this work in SAAG (for the time being)
  - Depending on the home(s) of other pEp related work move it as appropriate later-on

- Other suggestions?
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

Privacy by Default.