pretty Easy privacy

Short overview @ BFH, Oct 27 2017

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

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

p≡p

Privacy by Default.

Problem

- We have **Mass Surveillance**, now even widespread in countries we considered safe.
- We need **Mass Encryption** and **Mass Anonymization** to counter this.
- Citizens, enterprises and public offices have a right to be protected.

Problem

- Most messages nowadays flow between people like postcards → emails specifically.
- Email usage still grows: it won’t die. It’s the most important federated identity system.
- Messages should be encrypted and signed by default, for privacy and security reasons (e.g., phishing attacks).

Need for pretty Easy privacy

- “Good” privacy already exists (i.e., with PGP/OpenPGP implementations).
- **But:** Most users are not able to use email encryption tools like GnuPG (properly): its usability must be fixed through automatization.
- We need not just good, but **easy** privacy.
- We need **Privacy by Default**.

Philosophy: Cypherpunk & Privacy

“Privacy is necessary for an open society in the electronic age. [...]. A private matter is something one doesn’t want the whole world to know [...]. Privacy is the power to selectively reveal oneself to the world.”

Philosophy: Cypherpunks write code

"Cypherpunks write code. We know that someone has to write software to defend privacy, and since we can't get privacy unless we all do, we're going to write it."

Philosophy: Cypherpunks publish code

“We publish our code so that our fellow Cypherpunks may practice and play with it. Our code is free for all to use, worldwide.”

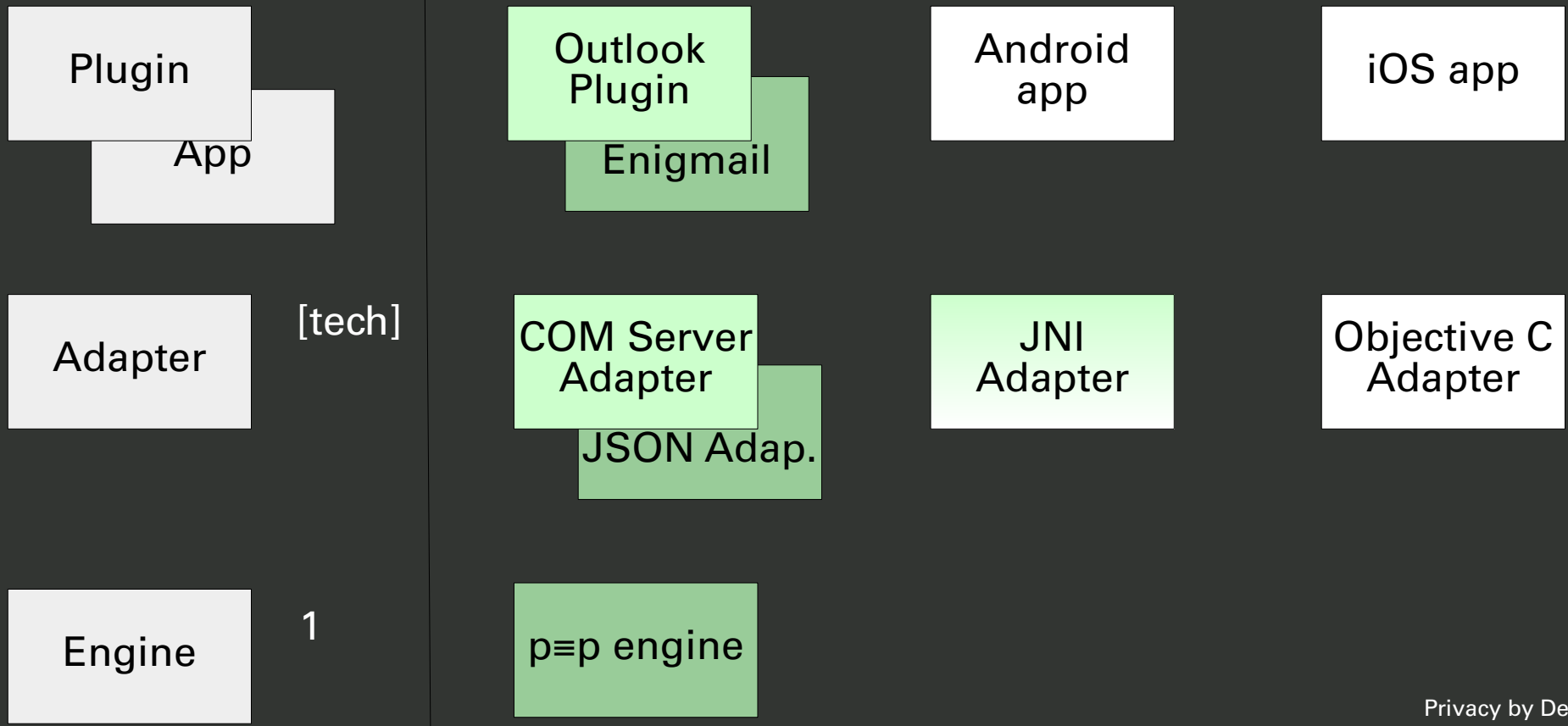
Approach of pretty Easy privacy

- Privacy by Default is achieved by writing code for automatization instead of manuals.
  - All code available under GNU licenses (as Free Software), cf. https://letsencrypt.pep.foundation/dev/
- Key pairs are created automatically for each account / URI.
- Public keys are distributed peer-to-peer (P2P) – for emails via attachment (and imported automatically by p≡p clients).

Approach of pretty Easy privacy

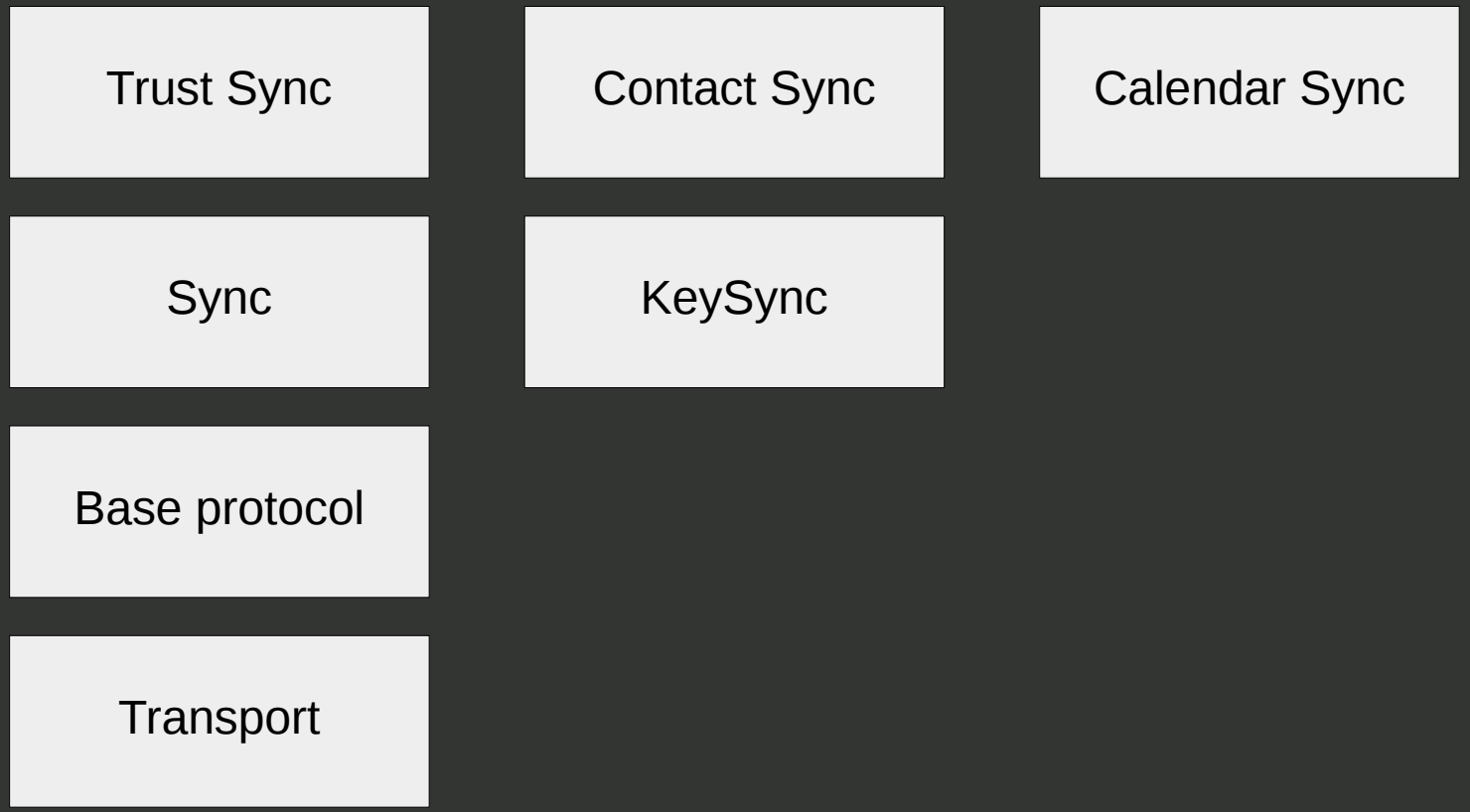
- No reliance on keyservers or centralized platforms.
- Identity verification is possible on a P2P basis through the use of Trustwords.
- p≡p stays compatible and thus is interoperable to existing standards (like OpenPGP).
- Furtherly p≡p, by principle, is agnostic to message transports and cryptography used.

p≡p software architecture



Privacy by Default.

Special feature: p≡p sync protocol



Questions

- ???
- ...
- Ask!