Privacy by Default.

p≡p

Privacy by Default.

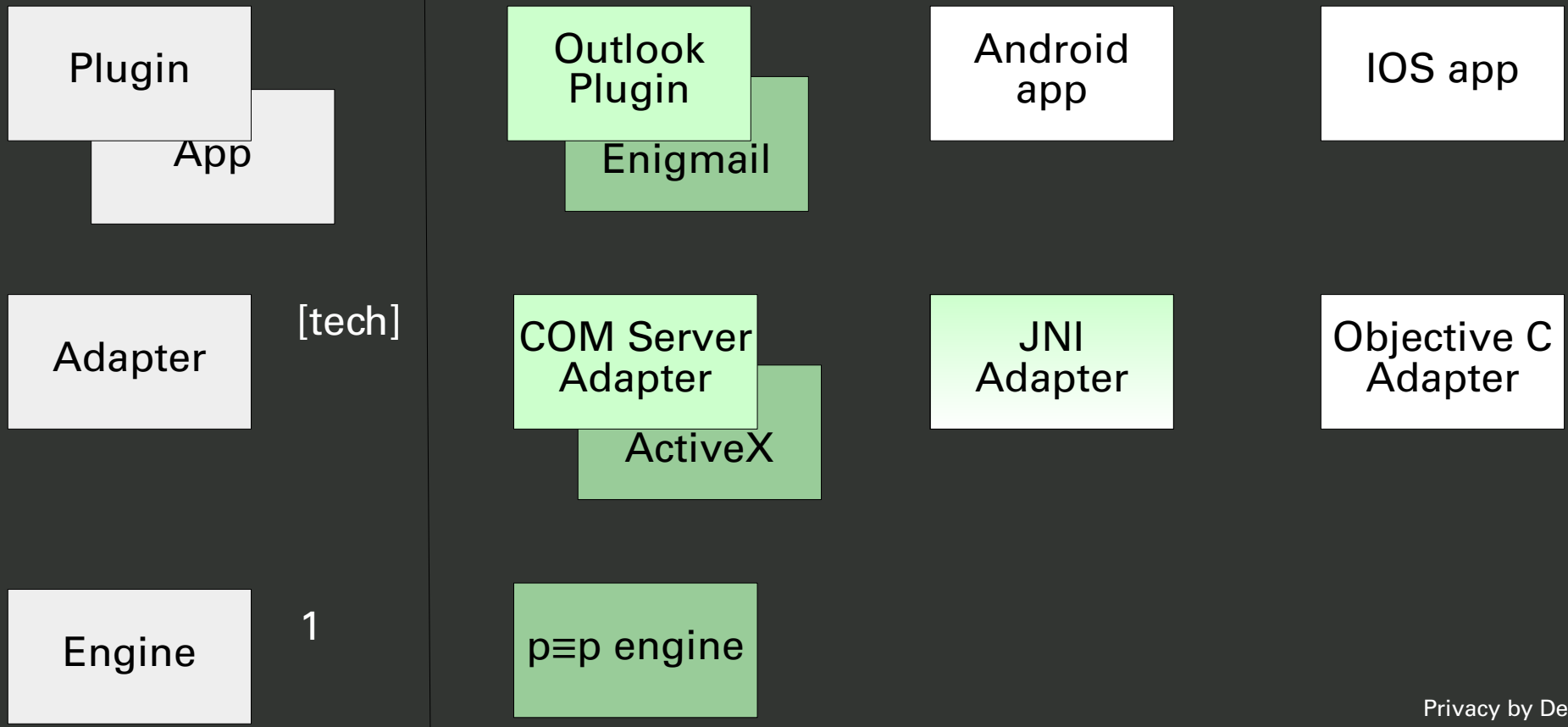
p≡p – the problem

- People are sending plenty of text messages
  - (i.e. Email, Jabber, …)
- Most people don’t understand Crypto at all
  - They don’t understand keys
  - They don’t understand signatures
  - They don’t understand the relation between privacy, confidentiality and crypto
- An implementation of Privacy by Default is needed
  - Taking away crypto needs from users’ view

Messaging platforms are easy…

- …Open Standards are not:
  - Interoperability vs. easy crypto implementations
  - Peer-to-peer Synchronization needed
  - Text message technologies are very different from each other
  - Crypto technologies for text messages are very different from each other
  - Client applications are very different, i.e. in Identity Management
  - “Will my message be kept private?” is a hard question to answer.

p≡p app architecture



Privacy by Default.

p≡p engine

Send-/ Receive | Message Loopback | Key-Manag. | Basic API | API

Crypto tech | Sync | Transport | MCR | abstraction

PGP (GnuPG) | (NetPGP) | OTR | GnuNET | Auto-transport | email | MIME | XMPP | low-level

NetPGP fork | Libetpan fork

Privacy by Default.

p≡p Sync protocol

Trust Sync

Contact Sync

Calendar Sync

Sync

KeySync

Base protocol

Transport

Privacy by Default.

Additions to IETF protocols

- Sync network protocol stack
  - Sync, KeySync, TrustSync, …
  - Base protocol mapping for email, Jabber, …
- Interoperability:
  - OpenPGP
  - S/MIME
- URI schemes for missing message addressing
  - mailto: irc: xmpp: are here, others are missing (like GNUnet Message Transport)

Additions to IETF protocols

- MIME based message formats
- Non-MIME based message formats
- Identity mapping
- Calendar mapping
- Key mapping
  - OpenPGP <=> S/MIME
  - Mapping on temporary symmetric keys

IETF: Help!

- Interoperability is most important for p≡p,
  so please help keeping it up
- We need critics and input for already implemented code and I-Ds (first draft submitted draft-birk-pep-00)
- Open Standards need management
  - Interfaces of Standards have to be kept working
  - p≡p can be an Open Standard itself (and should be)
- We need guidance where in the IETF this will fit?

Questions? BarBoF!

- Room Tyrolka, Mezzanine floor, today 19:30, including:
  - Demo of running code
  - Q & A
  - Discussion
- ... likely to be followed up in a bar close-by ;-)